S. HRG. 112–869

THE VIDEO PRIVACY PROTECTION ACT: PROTECTING VIEWER PRIVACY IN THE 21ST CENTURY

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY,
TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JANUARY 31, 2012

Serial No. J–112–59

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
87–342 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

AL FRANKEN, Minnesota, *Chairman*

CHUCK SCHUMER, New York	TOM COBURN, Oklahoma
SHELDON WHITEHOUSE, Rhode Island	ORRIN G. HATCH, Utah
RICHARD BLUMENTHAL, Connecticut	LINDSEY GRAHAM, South Carolina

ALVARO BEDOYA, *Democratic Chief Counsel*
ELIZABETH HAYS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

THE VIDEO PRIVACY PROTECTION ACT: PROTECTING VIEWER PRIVACY IN THE 21ST CENTURY

TUESDAY, JANUARY 31, 2012

U.S. SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:02 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Al Franken, Chairman of the Subcommittee, presiding.

Present: Senators Franken, Leahy, and Coburn.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator FRANKEN. This hearing will come to order. It is my pleasure to welcome all of you to the third hearing of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law.

Now, before we start, I just want to applaud the Supreme Court for its decision in the *Jones* case. It was, I believe, the right result, but it was also a call to action to Congress because, while law enforcement now needs a warrant to track your location, all of the companies that get your location information almost every day—your smartphone company, your in-car navigation company, and even the apps on your phone—are still in most cases free to give out your location to whomever they want, as long as it is not the Government. I have a bill to fix that, and I think we need to take action on it right away.

But today's hearing will focus on the Video Privacy Protection Act, a powerful privacy law that was written and passed by Chairman Leahy and Ranking Member Grassley of the full Judiciary Committee. I want to use this hearing to make sure that everyone knows what the Video Privacy Protection Act is and how it protects our privacy and our civil liberties. I want to look at how we might update the Video Privacy Protection Act for the 21st century, and I want to look at a specific bill to amend the law that was just passed in the House.

Twenty-five years ago, Judge Robert Bork was before the full Senate Judiciary Committee as a nominee to the Supreme Court. During that hearing, a local reporter asked Judge Bork's video store for a record of the movies he had watched. There was no law against it, so the video store gave him the records, and the reporter wrote a story about them. The Senate Judiciary Committee was

split on Judge Bork's nomination, but it was unanimous in its outrage over what had happened. There was not anything particularly memorable about Judge Bork's movie rentals. In fact, they consisted primarily of mysteries and caper films. But that was not the point. The point was that the movies we choose to watch are our business and not anyone else's.

Soon after this, Senator Leahy and Senator Grassley introduced the *Video Privacy Protection Act*. The bill was reported out of the Committee unanimously and passed through the Senate and the House on voice votes.

There has been renewed interest in the *Video Privacy Protection Act* in recent months, and I think that is great. But I have seen a lot of people talking about the law like it was some kind of relic, something that is so outdated that it does not make any sense anymore. So I want to take a moment to explain in simple terms what this law does for consumers.

Thanks to the *Video Privacy Protection Act*, your video company cannot tell other people what you are watching unless you give them permission to do that. Now, when Chairman Leahy and Senator Grassley wrote the law, they were really smart about it, if I might say. They did not just say that a video company has to at some point get you to sign some form that says, "I am OK with you telling people what I watch." No. They said that every time a video company wants to tell people what you watch, they have to check with you first. And that is an important right, because you probably do not care if people know that you watched some summer blockbuster. But if you are suddenly having trouble with your marriage and you are trying to get help, you might not want your friends and relatives to find out that you have been watching videos about marriage counseling or divorce. I also think that parents of a young child may want to watch documentaries about autism or developmental disabilities without broadcasting that to the world.

This can be really sensitive stuff, and that is why the *Video Privacy Protection Act* is so important. It gives you the right to tell your video company what can be shared and what cannot.

The *Video Privacy Protection Act* also protects your private sector against the government. Under the law, if the government wants to get your viewing records, it has to get a warrant, a grand jury subpoena, or a court order. This came up in one famous case where a local police department thought that the 1979 movie "The Tin Drum" was obscene. Now, mind you, this was a movie about what happened in Nazi Germany just before World War II. It won an Oscar for best foreign film. But the police department went out and seized a list of everyone who had the movie and then drove around confiscating every copy. And in that case, the ACLU chapter in the Ranking Member's State of Oklahoma used the Video Privacy Protection Act to stop that.

And so, without objection, I will add to the record a letter from the American Civil Liberties Union that stresses that this is a civil liberties law, too, not just a consumer protection law.

[The letter appears as a submission for the record.]

Senator FRANKEN. The *Video Privacy Protection Act* also makes sure that video companies do not keep information about what you

have watched after that information is no longer needed. This protects that information from getting lost, stolen, or hacked.

Finally, the law gives people the right to have their day in court to defend their rights if a video company or the government violates these rights.

So the *Video Privacy Protection Act* is a really important law for consumer privacy and for civil liberties, but things do change in a quarter century, and I am calling this hearing to see if we can update the law so that it can protect our privacy for another 25 years.

One way we need to update this law is to make sure that it is keeping up with technology. It used to be that if you wanted to watch a video, you had to go to the video store or then wait for it in the mail after that. Now you can stream it directly to your computer in seconds. Streaming is the future of video, but no judge has ever decided whether or not the *Video Privacy Protection Act* covers streaming video companies. I think it is clear that the law does cover new technologies like streaming because it does not just cover "prerecorded video cassette tapes." It also covers "similar audio-visual materials."

But I do think there is a real risk that a judge might look at this law and say it does not cover streaming, it just covers DVDs and VHS tapes and things like that. So I do not want to leave the future of video privacy up to a judge. So if we are updating the Video Privacy Protection Act, I think we need to confirm that it covers video streaming technology. I also know that the courts are split about whether or not people have the right to enforce the data retention provision. That might need to be clarified as well.

Those are just two ideas. I am sure the witnesses will have other suggestions. My goal here is to lay the groundwork for a fair and comprehensive update of the entirety of this law.

Before I close, I want to touch on H.R. 2471, a recently passed House bill that would modify one aspect of the *Video Privacy Protection Act*. H.R. 2471 lets a video company ask for your consent just once up front to disclose the videos you watch instead of asking for consent on a case-by-case basis. Netflix has strongly supported this bill and has explained that it will make it easier for them to integrate into social media sites like Facebook. I am pleased to report that Netflix is here with us today to talk about their support.

I want to be honest. Based on what I have seen so far, I have some reservations about H.R. 2471. First, it looks like the bill will basically undo users' ability to give case-by-case permission to a video company on what it can tell people and what it cannot. And that worries me because case-by-case consent, I believe, is a really good thing. It is a really good thing that people can easily tell their video company, "Sure, go ahead and tell people I watched 'The Godfather,' but, no, do not tell them I watched 'Yoga for Health, Depression, and Gastrointestinal Problems.' "

Senator COBURN. Is that one of——

Senator FRANKEN. Yes, for the record, that is a real title in the Netflix catalogue. And, by the way, it is an excellent film.

[Laughter.]

Senator FRANKEN. So I am worried that H.R. 2471 will eliminate our ability to give case-by-case consent, but I am also worried that

this bill will make these changes without confirming that streaming is covered or doing anything else to strengthen the law for consumers.

Finally, I want to know how this bill will affect the *Video Privacy Protection Act*'s protections against government snooping into our video records. But I am here to listen and to learn more about this, and this is a hearing on all proposals to update the *Video Privacy Protection Act*, not just H.R. 2471. And we have two great panels for that, but before I introduce them—do you want me to go to the Chairman first?

Chairman LEAHY. I tell you what. We have Senator Coburn here, and my——

Senator COBURN. I am happy to yield to the Chairman.

Chairman LEAHY. No, no. I will yield to you and also to—I know Congressman Watt, who has been such a leader in this, has to get back to matters in the House, so I will wait until after he has testified and, of course, I will follow the rest of you.

Senator FRANKEN. We will go to the Ranking Member, Senator Coburn, for his remarks. Thank you, Senator.

STATEMENT OF HON. TOM COBURN, A U.S. SENATOR FROM THE STATE OF OKLAHOMA

Senator COBURN. Mr. Chairman, thank you. I believe the Video Privacy Protection Act has become antiquated given all the new technology that is out there, and I would just note that you right now can share your music preferences through Spotify by setting up one time. You can share your book preferences by signing up one time. You can share your television programs through Hulu by signing up one time and news articles through Social Reader by signing up one time.

I think the Chairman of the Subcommittee makes some good points, and I am anxious to hear Congressman Watt and his thoughts on this. I did have a chance to talk to your Ranking Member yesterday and hear his input in it, and I look forward to the input.

Thank you, Mr. Chairman.

Senator FRANKEN. Thank you to the Ranking Member.

I think we will go to our first witness. That is what the Chairman would like, and what the Chairman would like, the Chairman gets. Our first witness is Hon. Melvin L. Watt, the distinguished Representative for North Carolina's 12th District. He has represented the people of the 12th District since 1992. Representative Watt serves on the House Judiciary Committee where he is the Ranking Member on the Subcommittee on Intellectual Property, Competition, and the Internet. Prior to his election to the House of Representatives, Representative Watt practiced civil rights law for more than two decades. He received his J.D. from Yale School and his B.S. from the University of North Carolina.

Representative Watt, welcome, and the floor is all yours.

STATEMENT OF HON. MELVIN L. WATT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Representative WATT. Thank you, Chairman Franken, Ranking Member Coburn, Senator Leahy, and Members of the Sub-

committee. I am truly honored to have this opportunity to address the Subcommittee about the amendments proposed in H.R. 2471 to the *Video Privacy Protection Act* and consumer privacy in this rapidly evolving Digital Age.

While I am the Ranking Member of the House Judiciary Committee's Subcommittee on Intellectual Property, Competition, and the Internet, the views I express here today are my individual views, and I do not speak for the Committee or the Subcommittee.

I believe there are countless reasons to oppose H.R. 2471, which relate both to what the bill does and what it does not do and how that fits into the broader debate about how best to protect individual privacy in the volatile online environment.

It is particularly timely that the Subcommittee holds this hearing today. Although online privacy has been at the forefront of discussion for the past few years, there has been a recent flurry of more intense discussion that I believe makes your hearing timely. Business leaders, consumer advocates, State and local elected representatives, and officials from each branch of the Federal Government have all weighed in with a variety of concerns and proposed solutions to address the absence of a uniform framework or approach to safeguard individual information in the thriving online environment.

Attention has appropriately intensified as two Internet giants, Facebook and Google, have come under scrutiny for their data uses, policies, and practices. Likewise, Netflix, the main proponent of this bill, has had more than its fair share of regulatory complaints and consumer lawsuits with regard to the handling of user information.

In the coming weeks, both the FTC and the Department of Commerce are expected to issue long-anticipated final reports on online privacy policy based on a series of roundtable discussions with relevant stakeholders and following up on their initial studies in 2010.

Senators Kerry and McCain in the Senate and Representative Cliff Stearns in the House last year introduced comprehensive legislation designed to prescribe standards for the collection, storage, use, retention, and dissemination of users' personally identifiable information, and these bills generated debate more generally in the halls of Congress.

This Subcommittee also held hearings to address the security of sensitive health records and personal privacy on mobile devices, and last week, in deciding whether GPS tracking violates a criminal defendant's Fourth Amendment right against unreasonable search and seizure, a majority of the Justices of the Supreme Court acknowledged the challenges we confront as a society in determining the so-called new normal for privacy expectations in the Digital Age.

Against this backdrop, I will direct the remainder of my comments to H.R. 2471, which passed the House under suspension of the rules. While I may not always avail myself of all the new technology and revolutionary tools and services available over the Internet, let me say at the outset that I applaud the explosion of technological advances that has transformed forever the way we communicate and transact business. While I support innovation on

the Web, however, I cannot do so at the expense of individual privacy. Given the gravity of issues involved, I believe it was a mistake for this bill to move through the House under the radar and without the benefit of a single hearing. But my concerns are not just about process. I believe that H.R. 2471 would have unintended negative consequences for consumers as well as affected businesses that will undoubtedly lose the confidence of their subscribers with the first privacy violation or data breach. Consumer desire to have access to the next cool tool should not be mistaken for the voluntary surrender of fundamental privacy interests.

In addition to the lack of thoughtful process in the House, I believe there are at least four substantive problems with H.R. 2471.

First, the bill leaves unaddressed the question of who the bill applies to, which I believe creates collateral, but important, intellectual property enforcement concerns. By declining to define what constitutes a videotape service provider under the VPPA, H.R. 2471 leaves open the possibility that businesses that provide video on demand over the Internet or those with dual distribution platforms like Netflix can avoid or delay compliance with legitimate discovery requests in copyright infringement actions.

Second, the debate on H.R. 2471 centered on the online experiences of consumers with social media like Facebook. However, the bill as passed applies to physical and online videotape service providers alike, and disclosures are authorized to any person, not on friends on Facebook. Consequently, a consumer's private information is vulnerable to release to third parties like the news reporter who published the video rental history of Judge Robert Bork that paved the way to enactment of the *Video Privacy Protection Act*.

Third, despite claims that the *Video Privacy Protection Act* is outdated, only a single provision of the statute was updated, leaving consumer-oriented provisions that should have been reviewed and strengthened unaltered.

Fourth, and finally, no consideration was given to the effect that changes in the Video Privacy Protection Act will have on State laws that afford similar and sometimes broader protections to consumers. This oversight is likely to invite thorny conflict of laws disputes given the borderless boundaries of the Internet.

While Internet users have a responsibility to self-censor and restrict the information they share about themselves, the reality is that many online users have a false sense of privacy due to their lack of understanding of lengthy and complex privacy policies they are compelled to agree to in order to use the service. As a result, online users often share a lot of personal information unknowingly and to unintended audiences. I do not believe that unsuspecting, unsophisticated, or casual Internet users should be deemed to relinquish their right to a basic level of privacy. And my concerns are heightened even more when the user is a vulnerable teen or young adult whose ability to adequately assess risk has not fully matured.

Third-party access to dynamic social platforms are constantly in flux. A consumer's consent today to allow perpetual access to their viewing history is clearly not informed by who will be their friend tomorrow. Today, when online bullying of teens and young adults can lead to depression or even suicide and online predators can learn otherwise confidential, private information about their prey,

I believe the selective and piecemeal amendment of the *Video Privacy Protection Act* is irresponsible.

As one commentator has written, movie and rating data contains information of a more highly personal and sensitive nature. The member's movie data exposes a member's personal interest and/or struggles with various highly personal issues, including sexuality, mental illness, recovery from alcoholism, and victimization from incest, physical abuse, domestic violence, adultery, and rape.

Justice Marshall wrote years ago that "Privacy is not a discrete commodity, possessed absolutely or not at all." The objective is to strike an appropriate balance to develop meaningful protections for consumers while promoting a healthy online economy. I do not believe that H.R. 2471 has found that appropriate balance. I support a comprehensive online privacy plan that will address and mitigate the unintended consequences of third-party sharing. In that regard, I believe Justice Alito got it right when he said: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."

This hearing is an important step toward finding the right balance, and it is more critically important because the House failed to give the matters the kind of attention they required.

I thank the Chairman for this opportunity and look forward to working across the Capitol to move forward. Thank you so much.

[The prepared statement of Representative Watt appears as a submission for the record.]

Senator FRANKEN. Thank you, Representative Watt, and the purpose of this is to give a hearing to all these matters and issues. Your complete written testimony will be made part of the record.

We are fortunate to have with us Chairman Leahy, who is the author of the *Video Privacy Protection Act*, and I understand that I left out Alan Simpson's role when I touted——

Chairman LEAHY. Alan was very important in that.

Senator FRANKEN. OK, so I apologize for that. He is a good friend. Today this law, the Video Privacy Protection Act, is just one of several critical privacy laws that the Chairman has written and passed during his tenure in the Senate, so I turn it over to the Chairman.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. I thank you very much, and it is good to see my friend Congressman Watt. We have worked together on so many things, from privacy issues to the Voting Rights Act, and I appreciate that collaboration.

I should tell Chairman Franken—and I thank him for his responsible leadership he has done on this issue of privacy—we Vermonters come about it naturally. I see a smile from a friend of mine in the audience who probably has heard this story more than once, but one of the few things I have ever saved written about me in the press—and I actually framed it—was a sidebar to a *New York Times* profile.

Now, to put this in perspective, you have to understand, my wife and I live in an old farmhouse in Vermont on a dirt road. We celebrated our—well, actually had part of our honeymoon there nearly 50 years ago, 50 years ago this summer. And hundreds of acres of land and fields that have been hayed and watched over by an adjoining farmer's family from the time I was a teenager, and they have known me since then.

So the whole story goes like this: On a Saturday morning, a reporter in an out-of-State car sees this farmer sitting on the porch and asks, "Does Senator Leahy live up this road?"

He said, "Are you a relative of his?"

He said, "No, I am not."

"Are you a friend of his?"

"No, not really."

"He expecting you?"

"No."

"Never heard of him."

Now, we like our privacy in Vermont. In the Digital Age, ensuring the right to privacy is critical. But I think it becomes ever more difficult as our Government and businesses collect and store and mine and use our most sensitive personal information for their own purposes—not ours, but theirs. Whether it is sensitive medical records, private financial information, or personal thoughts and feelings, I have worked, as so many others on this Committee have, to ensure that Americans' privacy rights are respected.

We talked about the *Video Privacy Protection Act* from 1988. When I introduced the bill, I said that it was intended to help make all of us a little freer to watch what we choose, without public scrutiny. More recently, I have worked at protections for library and book seller records in Section 215 of the *USA PATRIOT Act*.

Now, it is true that technology has changed, as the Chairman mentioned that Justice Alito said, but I think we should all agree that we have to be faithful to our fundamental right to privacy and freedom. Today the social networking, video streaming, the cloud, mobile apps, and other new technologies have revolutionized the availability of Americans' information. But they are also outpacing our privacy laws. That is one of the things we have to think about.

So I continue to push to enact the Personal Data Privacy and Security Act to create a nationwide data breach notification standard and better combat cyber crime. That is why I proposed a comprehensive review and update of the *Electronic Communications Privacy Act*.

Recently some companies that dominate various aspects of cyberspace have announced that they want to simplify matters so that they can more easily track Americans' activities across the board, obviously to their own financial benefit. But I worry that sometimes what is simpler for corporate purposes is not better for consumers. It might be simpler for some if we had no privacy protections, if we had no antitrust protections, if we had no consumer protections. It would be simpler for some, but it certainly would not be better for Americans. And I worry about a loss of privacy because of the claimed benefit of simplicity.

Privacy advocates and elected representatives from both sides of the aisle have serious concerns and serious questions. We are look-

ing for information and answers. When dominant corporate interests entice a check-off in order to receive what may seem like a fun new app or service, they may not be presenting a realistic and informed choice to consumers. A one-time check-off that has the effect of an all-time surrender of privacy does not seem like the best course for consumers. I worry that the availability of vast stores of information via corporate data banks also makes this information readily available to the government, which has almost unfettered power to obtain information with an administrative subpoena and so-called national security letters. So I think we need to have comprehensive reform.

Now, Representative Mel Watt is a thoughtful leader on these issues, and it is good that he is here, as well as those from corporate America. But I am hearing from many privacy advocates who have expressed concern about the privacy implications of the House-passed proposal. A key concern is that a one-time check-off of consent to disclose, mine, sell—sell, sell—and share information does not adequately protect the privacy of consumers. And the House's proposal updating the law does not cover streaming and cloud computing to the extent I would like. So we need to move forward with a comprehensive review and update of the *Electronic Communications Privacy Act* and also see how best to update to the *Video Privacy Protection Act*.

I want to thank the Chairman for doing this, and I just want to stress again that this Vermonter likes his privacy. And I especially do not like it when somebody says, "We are just going to make life simpler if we sell your privacy."

Senator FRANKEN. Thank you, Mr. Chairman.

We are now going to go to the second panel. Thank you again, Representative Watt. You were the first panel. Evidently a single person can be a panel.

Senator FRANKEN. If the panel would come forward, I would like to introduce our second panel of witnesses.

David Hyman is the general counsel of Netflix. Mr. Hyman has served in this role for the past decade and has seen the company grow tremendously during that period. Prior to joining Netflix, Mr. Hyman was the general counsel of Webvan, an Internet-based grocery delivery service. He received both his J.D. and B.A. from the University of Virginia.

Bill McGeveran is an associate professor of law at the University of Minnesota, where he specializes in information law, including digital identity and data privacy. Before joining the university, he was a resident fellow at Harvard's Berkman Center for Interest and Society and a litigator in Boston. Professor McGeveran received his J.D. from NYU and his B.A. from Carleton College in Minnesota. Finally, I should add that Professor McGeveran was once a staffer for Senator Schumer back in the days in the House of Representatives.

Marc Rotenberg is the executive director of the Electronic Privacy Information Center, which he co-founded in 1994. He chairs the American Bar Association Committee on Privacy and Information Protection and has edited several privacy law textbooks. Prior to founding EPIC—that is, again, the Electronic Privacy Information Center, EPIC—Mr. Rotenberg was counsel to Senator Leahy,

where he advised the Senator on the law that we are considering today, the *Video Privacy Protection Act*. He received his J.D. from Stanford Law School and his B.A. from Harvard College.

Christopher Wolf is the director of the privacy and information management practice at Hogan Lovells here in Washington, and he is also the founder and co-chair of the Future of Privacy Forum. He was the editor and lead author of the Practicing Law Institute's first treatise on privacy law and has authored numerous publications on privacy. He received his J.D. from Washington and Lee University and his A.B. from Bowdoin College.

I want to thank you all for being here today. We will start with Mr. Hyman.

STATEMENT OF DAVID HYMAN, GENERAL COUNSEL, NETFLIX, INC., LOS GATOS, CALIFORNIA

Mr. HYMAN. Chairman Franken, Ranking Member Coburn, thank you for the opportunity to testify today on the *Video Privacy Protection Act*. My name is David Hyman. I have served as the general counsel of Netflix since 2002: a time when streaming video over the Internet to a "smart" TV was more the stuff of a sci-fi miniseries than a topic of serious consideration in a board room, much less a Congressional hearing. How far we have come in such a short period of time. Today's hearing is a testimony to the incredibly dynamic and powerful innovation engine of our Internet economy.

Netflix was founded in 1997 as a DVD-by-mail service. To many, the use of the Internet and the Netflix Web site was nothing more than a way to submit orders for physical disc delivery. But for Netflix, we saw an opportunity to use technology in a way that helped consumers discover movies and TV shows they would love, as well as provide business opportunities for content producers and distributors. The popularity of our DVD-by-mail service grew rapidly. But with innovation deeply rooted in our corporate DNA, we continued to research and try new and compelling consumer offerings. We were an early pioneer in the streaming of movies and TV shows over the Internet to personal computers. And in 2008, we began to deliver instant streaming video to televisions through the use of a handful of Internet-connected devices. Today, more than 21 million consumers in the United States use the Netflix streaming service on more than 700 different types of Internet-connected devices, including game consoles, mobile phones, and tablets. And in the last three months of 2011, we delivered more than two billion hours of streaming movies and TV shows to those consumers.

At the same time that the Netflix streaming service has seen such uptake by consumers, the world of social media has exploded in popularity. Embodied by the growth of Facebook, the social Internet offers tremendous opportunities for consumers and businesses. Netflix believes that social media offers a powerful new way for consumers to enjoy and discover movies and TV shows they will love. To this end, we have been offering our members outside the United States the opportunity to share and discover movies with their friends through the Facebook platform. While it is early in the innovation process, we have seen strong consumer interest in

our social application, with more than half a million subscribers outside the United States connected with Facebook.

Unfortunately, we have elected not to offer our Facebook application in the United States because of ambiguities in the Video Privacy Protection Act. Under this law, it is unclear whether consumers can give ongoing consent to allow Netflix to share the movies and TV shows they have instantly watched through our service. The VPPA is an unusual law; unlike most Federal privacy statutes, the VPPA could be read to prohibit consumers who have provided explicit opt-in consent from being able to authorize the disclosure on an ongoing basis of information they so desire to share. The friction that this ambiguity creates places a drag on social video innovation that is not present in any other medium, including music, books, and even news articles.

Recognizing this, the House recently passed a bipartisan bill, H.R. 2471, that clarifies consumers' ability to elect to share movies and TV shows they have watched on an ongoing basis. H.R. 2471 leaves the opt-in standard for privacy within the VPPA undisturbed. Netflix supports the opt-in standard and believes that this approach is workable and consistent with our members' expectations and desires.

The VPPA singles out one type of data sharing. Instead of trying to graft specific notions about video privacy from almost 25 years ago into the dynamic information age of today, we would encourage a measured and holistic review of privacy for the 21st century, one designed to foster continued innovation while balancing the desires and privacy expectations of consumers. Such a review will understandably take considerable time and effort, and we are ready to assist. In the interim, it is our hope that the Senate will see the value in clarifying the right of consumers to opt in to ongoing sharing under the VPPA and quickly approve H.R. 2471.

Again, I thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Mr. Hyman appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Hyman.

By the way, your complete written testimony will be made part of the record.

Professor McGeveran.

STATEMENT OF WILLIAM MCGEVERAN, PROFESSOR, UNIVERSITY OF MINNESOTA LAW SCHOOL, MINNEAPOLIS, MINNESOTA

Mr. MCGEVERAN. Thank you. Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee and staff, thank you for inviting me to testify here today.

My name is William McGeveran. I am a law professor at the University of Minnesota. My teaching and research focus on Internet, privacy, and intellectual property law. In that context, I have written about the *Video Privacy Protection Act*, which I consider a model for privacy legislation more generally.

Now, unquestionably, there are enormous benefits to the online recommendations we get from friends through sources like Facebook or Spotify, and I myself use social media and those rec-

ommendations heavily. But the potential problems are serious too, as others have noted. In one article, I argued that the key to getting that balance right is securing genuine consent. That means an individual sent a social message intentionally, not by mistake. If we have too many accidental disclosures, we undermine the privacy of personal matters and also the accuracy of the recommendations, the fact that our friend really wants us to see this movie rather than passively letting us know that he saw it and it turns out maybe he did not like it very much. The VPPA is designed to secure that sort of genuine consent.

I want to emphasize three points: first, the important interests behind the VPPA; second, the fact that amendments are not necessary to keep up with technology; and, finally, the problems with H.R. 2471.

First, the VPPA safeguards important interests, as others have noted. Why else did a newspaper reporter think Judge Bork's rental history might be interesting in the first place except that it would be revealing of something about him?

In my view, the greatest flaw in the existing VPPA is its limitation to video, which arises from a historical accident around its enactment. Unintended disclosure of a user's choices of books, music, films, or Web sites can also constrain the capacity to experiment and explore ideas freely. If the Committee revisits this statute, I believe you should consider extending protection to reading and listening habits as well as viewing. That was part of the intent of the California Reader Protection Act, which took effect at the beginning of the month. In general, the law ought to protect private access to any work covered by copyright, not just movies.

Second, the VPPA, in its current form, already allows video companies to implement social media strategies, including, if they wish, integration with Facebook. Now, it is true that the VPPA requires opt-in consent every time a viewer's movie choices get forwarded to a third party, and that includes friends in a social network. That is not an ambiguity. That is actually clearly what the law says.

But it is actually easier to satisfy those requirements online than off. The statute's authors, after all, such as Senator Leahy, envisioned a video rental store getting the customer to sign a separate document with pen and paper every time in person. On the Internet, by comparison, each time users push the button to play a movie, they could be offered a "play and share" button right alongside it allowing them to both show the video and post that information in social networks.

I think it would be quite radical to assert that an electronic format does not fulfill the requirement for written consent under the statute. That interpretation would undermine every clickwrap and "I agree" button that is on the Internet. It is contrary to the *E-SIGN Act* and to all the case law I have seen.

I think the real objection here is not about technology. It is a disagreement with the VPPA's explicit policy choice to get case-by-case consent rather than a one-time authorization.

Finally, I do want to note that H.R. 2471 has a lot of problems and misses some opportunities for reasonable compromise. I will just note a few.

Changes to the statute apply to every disclosure, not just those in social networks. By rushing to address Netflix and Facebook, the bill reduces privacy in many other settings, from law enforcement to behavioral advertising. By specifically mentioning the Internet, I am concerned the bill may foreclose electronic consent through other technologies such as cable or satellite, and that is a real concern.

The provision for withdrawing consent says nothing about how it is supposed to be done. That vagueness may, apparently, permit companies to comply by making it easy to give consent but very cumbersome to withdraw that consent.

Most important, the bill passed by the House replaces a robust consent provision with a very weak alternative. There may be other ways to get genuine consent than what is offered in the VPPA. For example, what about general authorization with a short time limit, say one month, and granular, clear opt-out for individual postings? I urge the Committee and the bill's supporters to explore those sorts of creative compromises to streamline the VPPA for the 21st century without vitiating its important protection for individual privacy.

Thank you, and I look forward to questions.

[The prepared statement of Mr. McGeveran appears as a submission for the record.]

Senator FRANKEN. Thank you very much, Professor.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC

Mr. ROTENBERG. Mr. Chairman, Senator Coburn, thank you very much for the opportunity to testify today.

As you know, there are few issues of greater concern to Internet users than the protection of privacy. In fact, according to the Federal Trade Commission, over the past decade the top concern of American consumers has been privacy and identity theft, so the hearing that you are holding today is very important, very timely, and of great concern to a lot of people.

I wanted to begin by talking about the purpose and passage of the *Video Privacy Protection Act*. As you suggested, Mr. Chairman, in many ways this was a smart and forward-looking piece of legislation. Among the various provisions that Congress enacted 25 years ago was one that said let us not keep personal information longer than is necessary. Today we have an enormous problem in this country with data breaches, identity theft, and companies keeping data on their customers and their clients for much longer than they should. Fortunately, in this area there are strong safeguards that have prevented and protected users of these new services from those types of problems.

What the *Video Privacy Protection Act* sought to do was to deal with the new reality in video services. Prior to the mid-1980s, as you know, most people watched broadcast television or saw movies. There was very little collection of personal data about individuals' particular movie preferences. And so when the story broke about the access to Judge Bork's video rental records, Congress appro-

priately said we need to put in place some safeguards for that information that businesses were now able to collect.

Now, the act establishes a strong presumption in favor of privacy, but it is not a prohibition against disclosure. Individuals always have the right to consent to disclosure. Law enforcement has the right under a court order to get access to records in the course of an interrogation. And even for marketing purposes, personal information can be disclosed, and this is the key provision that I would like to draw your attention to, because there was an important compromise that the Congress struck when they were considering the act. They said when it comes to the fact that someone may happen to be a customer of a video service, there really should be few restrictions on disclosing that fact, and the privacy protection was essentially an opt-out. Congress even said that if the company wanted to disclose the fact that a person was interested in science fiction movies or mystery movies or action adventure, companies in those circumstances as well could disclose those facts simply with the opt-out protection.

But when it came to the actual titles of particular movies that would reveal so much about a person's personal interests and the likes, Congress said, well, there we need a higher level of protection. That should really be opt-in. And if a person chooses in a particular case to disclose that information, they should be free to do so, and the act allows for it.

Now, I want to say very directly to Netflix that this argument that they are making that this law somehow stands in the way of integration with Facebook is simply not right. They have the freedom today under the law to note when Netflix users are using Netflix services. They can even go the next step and talk about the types of movies that their customers are viewing. What the law tries to do is establish a line at the point that the company wants to say, "And here is the particular movie that one of our users is now viewing." That is where the law says, please, in those circumstances, get opt-in consent.

Now, I want to make a further point here because I actually believe that many of the House members who voted for this bill do not fully understand the consequence of the amendment. It is not just the friends of that individual to whom the fact of the specific movie viewing will be disclosed. It is also to Netflix business partners, and it is also potentially to law enforcement, because what Netflix is asking users to do is to provide a blanket consent that gives them the opportunity to disclose specific movie viewing to any party under any circumstance that Netflix chooses to. This knocks out the cornerstone of the act. It takes away the key provision that was put in place to give users meaningful consent.

Obviously, I do not think this is going to support online privacy and, frankly, I do not think Netflix users want this provision. But I do think changes could be made to the act to modernize it and to update it. I think it should be applied to all streaming services. I think that data destruction provision needs to be coupled to the private right of action. I would also like to see more transparency so that users of the service actually know how their personal information is being used, and I think companies should be required to routinely encrypt the data they collect. Those types of changes to

the act actually would update it, would continue to promote a viable and useful service for many users, and I hope they will be considered by the Committee.

Thank you.

[The prepared statement of Mr. Rotenberg appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Rotenberg.

Mr. Wolf.

STATEMENT OF CHRISTOPHER WOLF, DIRECTOR, PRIVACY AND INFORMATION MANAGEMENT GROUP, HOGAN LOVELLS LLP, WASHINGTON, DC

Mr. WOLF. Thank you, Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee. My name is Christopher Wolf, and I am a privacy lawyer at Hogan Lovells, where I lead that firm's global privacy practice. I am also a privacy advocate. As part of my pro bono work, I won a leading case against the government for violating the Electronic Communications Privacy Act. I am part of a group advising the OECD on its privacy guidelines. I am on the EPIC Advisory Board, and I founded and co-chair the Future of Privacy Forum, a think tank with advisory board members from business, consumer advocacy and academia, focused on practical ways to advance privacy. I am pleased that Professor McGeveran is a member of that advisory board.

Fundamentally, privacy is about control. Indeed, a principal goal of privacy law is to put choices and decisions in the hands of informed consumers. With the advent of video streaming and social sharing, the Video Privacy Protection today stands in the way of consumers' exercising control and, thus, limits their choices and even limits free expression.

The VPPA, enacted nearly a quarter of a century ago during the Betamax era, was designed to prevent prying into people's video rental history. The purpose of that law was not to stop people from sharing information about the videos they watched or to dictate how they share. Indeed, the law's laudable purpose was to give control and choice to consumers, to let the consumers decide whether and how to share their video-watching information.

In 1988, when the VPPA was enacted, no one dreamed of streaming video and social sharing. So when that pre-Internet era law is applied to the world of online video and social media, it can be read to frustrate the choices of consumers to authorize the disclosure on an ongoing basis of the streaming movies they have watched online.

For many people, automatic sharing in social media is how they shape their online identities and how they share ideas. Facebook users commonly utilize a one-time authorization, a durable sharing option, to share a wide range of information with their friends. But when it comes to sharing their online video experiences, the law gets in the way.

Take a person who is an avid video watcher watching 100 short videos per week. She wants to share every video she watches with her friends, just as she shares every song she listens to on the streaming music service Spotify and just as she shares every item she reads online on the *Washington Post* through a Facebook social

sharing app. But current law suggests she is not fit to make the frictionless sharing decision with respect to videos she watches. Should this video file have to opt in 100 times per week? Does making her do so serve any purpose other than to annoy her and to take needless time? The constant, legally required interruption to her online experience harkens back to the day when pop-ups had to be clicked on to proceed online. Our frequent video viewers should be given the opt-in choice to share all of her viewing experience if that is what she wants.

In contrast to the restrictions of the VPPA, there are no legal restrictions on her ability to socially share every e-book she reads. Through a durable sharing option, she easily can share the fact that she read the book entitled "The Godfather," but the law stands in the way of her similarly sharing the fact that she watched the movie entitled "The Godfather." That makes no sense.

Of course, not everyone wants to share their viewing experiences with their friends online, and they do not have to share. And if someone prefers to share their video-watching experiences on a case-by-case basis, he or she can do so manually, just as people occasionally post news stories they read on the *Washington Post* on Facebook rather than choosing the automatic sharing option.

Similarly, a person who chooses to share on a continuous basis can disable the share function before watching a streaming video that he or she wants to exclude from online post, such the "Yoga for Health" video that Senator Franken referenced.

In order to clarify the uncertainty of the language in the VPPA on disclosures, I support an amendment such as H.R. 2471 allowing durable sharing choice for consumers, which in turn will permit frictionless social sharing. I agree that as a privacy best practice, the durable choice option should be opt in and presented prominently, separate and distinct from the general privacy policy and the terms of use of an online service. That is genuine consent.

I join the Center for Democracy and Technology in concluding that such an amendment will not undermine the fundamental purpose of the VPPA. Even though some Senators personally may feel that sharing all the movies one watches is, to use a phrase not heard much anymore, TMI, too much information, people should as a matter of free expression be able to share as they choose, and companies should not face legal penalties for providing them with that choice.

As governments around the world, including our own, consider ways to improve their privacy frameworks, there are big decisions to be made, as Representative Watt pointed out in his presentation. Starting a legislative process in the name of privacy protection through which lawmakers decide case by case what information and by what means consumers can share online seems terribly ill-advised. In contrast, amendment of the VPPA to permit full user choice and control fits squarely within the preferred privacy framework, one that empowers consumers.

Thank you for the opportunity to appear here today. I look forward to your questions.

[The prepared statement of Mr. Wolf appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Wolf, for your testimony.

Let me start with Professor McGeveran because I want to make a few things clear about what this bill does and does not do. I talked a little in my opening statement—or about what the amendment does and does not do, about what the video—I talked about what the Video Privacy Protection Act does. I want to talk for a moment about what it does not do. A lot of people have been saying that the Video Privacy Protection Act actually prohibits people from sharing their viewing habits on social networking. In fact, one article said that, "An antiquated 1988 bill called the Video Privacy Protection Act forbids the disclosure of one's video rental information even if the renter is OK with the disclosure."

Is that right, Professor McGeveran? Does this law prevent—and I am talking about the VPPA—video companies from integrating into Facebook or other social networking sites even if the user wants them to?

Mr. MCGEVERAN. No, it is not right, Senator. The underlying existing statute, which I am concerned it is called "antiquated" since that is the year I graduated from high school. But the statute requires consent every time. But as I mentioned in my opening statement, that can be done simply by saying here is a button to press when you play the movie, because presumably you have to press a button to play the movie, and right next to it here is a button to both play and share. You can post. You just have to be asked every time you see a movie online. That seems relatively easy to effectuate.

Senator FRANKEN. So it would be easy to say I can share.

Mr. MCGEVERAN. That is right.

Senator FRANKEN. Mr. Wolf talked about it would be really easy to disable the sharing, but is there anything in the amendment that says how that would happen? Could an online video company, one less scrupulous than Netflix, just have it really hard—is there anything in the law that would prevent them from making it almost impossible to figure out how to disable it?

Mr. MCGEVERAN. In the House bill, the way it is set up now, it says that you could enable consent until you took it away, but there is nothing in the bill that gives any requirements about how that would be done.

Mr. Wolf mentioned some best practices. You know, I think a scrupulous company would make it easy. But this law is not only going to apply to companies that we believe are going to do the right things, and it does not—the company could have no button or access anywhere on its Web site to do this. It could perhaps have no explanation on its Web site that you had the right to do this, and it would be up to the consumer to figure it out. And the House bill allows that kind of arrangement.

Senator FRANKEN. OK. I just want to make that kind of clear, that to opt in to sharing a video, what movie you are watching, would be no more burdensome than just watching the movie itself.

Mr. MCGEVERAN. Under current law.

Senator FRANKEN. So, in other words, press one button. However, disabling the overall consent to watch everything could be impossible to find, essentially.

Mr. MCGEVERAN. That is right. The House bill does not——

Senator FRANKEN. Mr. Rotenberg, do you agree with that?

Mr. ROTENBERG. I think this is a very important point, Senator, and also what Professor McGeveran has pointed out is that there are innovative ways to allow individuals to click, you know, "play and share". There is the integration, and there is the disclosure, or to simply click "play," which is I just want to see a movie, I do not need to tell the world about it. But the point that you are making which is of particular concern to us is under the House approach, once you basically have "play and share stuck," that button setting, it may be very difficult to unstick because there is nothing in the proposal that would make it easy to withdraw the consent.

Senator FRANKEN. OK, thank you.

Mr. Hyman, there is no company that better exemplifies the promise of streaming than Netflix. Netflix introduced its streaming in 2008. Today 90 percent of Netflix's 24 million subscribers have streaming subscriptions; only 45 percent have DVD subscriptions, and that number is dropping. In fact, if you look at "About Us," the "About Us" section on Netflix's Web site, the word "DVD" does not appear once. It is all about streaming, and for good reason, because that is the future of video.

I mentioned in my opening statement that there may be some disagreement as to whether or not streaming video companies are covered by the *Video Privacy Protection Act*. Mr. Rotenberg suggested in his testimony that it would be helpful to change language in the *Video Privacy Protection Act* to confirm that it does, in fact, cover streaming video companies.

Mr. Hyman, would Netflix support doing that?

Mr. HYMAN. Mr. Franken, Netflix would probably not—we would not support that. I think the issue for us is really one of what is video in the future and how do you think about that in the Internet age. Video embedded into news stories, does that become a news story or is that streaming video? Music videos, is that music or is that videos? Books. You know, I recently read a book called "A Visit from the Good Squad," which is a very good book. Interestingly, it uses in there texting. It has a PowerPoint presentation. You can imagine in the future that books will incorporate video. Does that now mean that that is covered by the VPPA?

So I think we have a host of issues relative to what is video in the future, and so just extending the Video Privacy Protection Act into the Internet raises a host of issues, and I think there is a host of other players that need to be involved in that.

So, again, as we mentioned in the testimony, a holistic approach and a comprehensive approach would be one that Netflix would support and be involved in, but merely taking the VPPA and saying it applies to streaming, I think, opens a whole host of issues that need to be carefully addressed.

Senator FRANKEN. Would anyone care to address that in terms of—because I do not think this amendment is comprehensive at all. And so I think you raise a lot of great issues about this, but it seems to me to say that since the VPPA applied to what we think of as movies, movies are going to be streamed.

Mr. HYMAN. They are.

Senator FRANKEN. They are going to be. So that this law, it seems like that you need to apply streaming to this, and I am troubled by your excluding, trying to exclude streaming at all.

Does anyone have anything to say about that?

Mr. ROTENBERG. Well, Mr. Chairman, I think perhaps the advocates of that approach are drawing the wrong line. The *Video Privacy Protection Act* was not trying to regulate technology. It was not saying we will treat, you know, video rental cassettes in one way and other things in a different way. It actually says similar materials should be treated in a similar way.

What the act is trying to do is regulate the collection and use of personally identifiable information, and the reason you need to do that in the digital world is because when you move from broadcast of television and movies to this kind of one-to-one service offering, these companies are now collecting a lot of personal information about their customers. And so what the law tries to do is to say if you are going to collect all that data, then you need to protect.

And I think the other point that should be brought out as we think about these new techniques for delivering of video is that companies today are collecting a lot more information than they did 25 years ago. And so I would think that the inclination at this point in Congress would actually be to strengthen the law, recognizing how much more information is collected.

Senator FRANKEN. Well, thank you. We will go to another round. I have run over my time. We will go to the Ranking Member, Senator Coburn.

Senator COBURN. First of all, let me thank you for your testimony. I learned a lot from what you had to say. And I am prone to agree with the Chairman on his concerns about this bill as I look at it. And I really do not see a big difference from granting permission one click at a time to a blanket consent. But I also think prudence in terms of protection of privacy ought to be the thing that ought to guide us.

There is no question Netflix with their policy throughout the rest of the world that is not available here to online consent for that gives them an asset, my asset, my privacy asset, that I readily give to me if I am one of those that grants a blanket consent somewhere outside this country. I am giving them something of value that they can use to make money off of. And I am not sure—I am torn between whether we have the right to tell somebody whether they can grant a blanket consent or not. I do not know that that is our role. But I know it is our role to be concerned about the ultimate privacy protection that individuals deserve.

So I would go back and I would ask the professor if he would give us a little further dissertation on what he thinks or means by the words "genuine consent."

Mr. MCGEVERAN. Thank you, Senator Coburn. The idea behind genuine consent is to say that it is thought out, it is intentional. We are helping a consumer, a customer, to post the information that he or she wants to post.

I might have more sympathy toward changing the existing VPPA if I thought it did, in fact, make it very difficult for people to do that, because I think that recommendations of movies to our friends are really valuable. I learn a lot about movies I would like to see by hearing about them word of mouth from my friends. But as I mentioned before, what we have online is the capacity to make it very easy to secure a decision each time from the user, to say

yes, I do intend to share this information now about this movie now. And the ability to say it for all movies in advance, we are not actually inconveniencing the user very much in an era where you are going to have to push either just one button or the other. So I would say genuine consent is making sure that it is intentional.

Senator COBURN. So when I go through Dallas airport and use Dallas' wi-fi, at the bottom of that every time is "I consent," I agree to their terms. Now, how many of you in this room have ever read that three pages of very fine print to say you agree to consent?

Mr. MCGEVERAN. Well, I have, but that is my job.

Senator COBURN. Yes.

[Laughter.]

Senator COBURN. But you are a rarity.

Mr. MCGEVERAN. I am.

Senator COBURN. And so the fact is, what you are saying is what is wrong with making a considered judgment each time.

Mr. MCGEVERAN. Exactly.

Senator COBURN. Mr. Wolf.

Mr. WOLF. Senator, I think you pointed out the problem with that, that when consumers are presented with choices over and over and over again, they tend to tune them out, and they will ignore them, and they will have no meaning whatsoever. They will just click through it to get to the function that they want to exercise.

Senator COBURN. Well, let me bring you back to this point. If the question that comes up on my iPad is, Do you want to share this information through your social media?, and I have to say yes or no, that is all that is going to be required for Netflix to put up with each movie: Do you want this to be shared? You have to make a decision there. That is a one-line statement, which is very different. So if I am looking at a movie, an Arnold Schwarzenegger, which my wife hates but I love the action in them, and I am going to make a decision that I want everybody to know I am watching Arnold Schwarzenegger, and I am going to have to—it is one sentence. I am going to have to make that decision. Why is that not protecting the rights rather than blanket, and, "Oh, I forgot about it," or "I am hung over from the night before, and I am not thinking clearly," so, therefore, I have already granted—and I punched a button on something that I really do not want shared.

The question is: Should we err on the side of privacy, or should we err on the side of commerce? And that is the real rub here. That is the thing that we have to decide.

Mr. WOLF. I actually do not think that is the choice. If a consumer wants to share everything on their Facebook page, as many do—they share every article they read in the *Washington Post*, every book they read, every song they listen to. It is not a choice you or I might make, but a law that takes away that choice really ignores that there are people who want to do that. And as long as they are informed of the consequences of doing that and provided an opportunity—and I agree with the professor that the opportunity ought to be just as easy as it is to opt in—then I really do not see how it is the business of Congress to dictate how and when people share.

Again, we are talking about legislating today, but we have no idea what the sharing techniques will be 20 years from now. And I will leave this to Mr. Hyman, but I understand that there are some devices to access Netflix where you cannot have that button or it is not easy to have that kind of button that you are talking about.

Senator COBURN. That is fair. The point is there is a rub. There is a rub. And the argument is not simply that we are going to take away somebody's right to share. And it is not being a Big Brother. I will go back. I believe the decision is between protecting privacy and promoting commerce, and I think we ought to be able to figure out how to do both.

Mr. WOLF. But I get back to my fundamental point, that privacy is and has all along been giving people the choice to control their information and who sees it and how it is disclosed.

Senator COBURN. So there is no limitation to that choice if I get to make that choice each time. You are still giving them the choice. You are still giving—actually, we had a reference to the testimony that some think that the ability to use Spotify right now ought to have a choice each time. Is that not true? Did I not get that inference from your statement, Mr. McGeveran?

Mr. MCGEVERAN. Spotify is not set up in a way that would be compliant with the VPPA if it were video because your scroll of songs is sent out to all your friends automatically.

Senator COBURN. Yes, but the point is, was it not your inference that you thought maybe people ought to be making decisions on that as well?

Mr. MCGEVERAN. That is right. I think the same thing, you press a "play" button for a song, you should be making a choice time by time whether that is something that goes out.

Senator COBURN. So the question is how big of a choice do you make and whether you reconsider it. The question I would have technically is if I opt in for all of it, each time Netflix brings me a movie, do I have the option to opt out of that? In other words, do I have a default button that goes out?

Mr. WOLF. Again, I think the opt-out option ought to be easy, but, you know, there are people who have webcams and they leave them on all the time, and some people think that is ill-advised, they are oversharing, it invades their privacy. Imagine a law that Congress passes that says that the webcam as a matter of law will be turned off once every 24 hours, and you have to make the choice to turn it back on. That just has never been the business of Congress to tell people how they publish, how they share, and with whom they share. Privacy is about allowing people that choice.

Senator COBURN. Again, I do not say your arguments do not carry large weight. I am just saying in terms of effectuating the protection of privacy, how are we going to do that? Let us say we go to this and we are going to have an opt-in. Where are the details on the opt-out?

Mr. WOLF. Well, I agree, that needs to be——

Senator COBURN. It is not in there.

Mr. WOLF. That needs to be specified. But I really caution against the slippery slope of controlling every kind of information and every kind of technology in terms of how people share.

Senator COBURN. We are not controlling it. What we are saying is you got to make a choice, and, you know, the question——

Mr. WOLF. But only the choice you want them to make, not the choice that is available as to other information.

Senator COBURN. No, no. There are two choices: opt in or opt out. The point is you got to still make the choice with your privacy, and I think there is a legitimate concern that if you opt in, will you have the same presence and available information to opt out. So the question I would have of Netflix is, if you have this or where you have it in Europe, does somebody every movie have an opportunity to opt out?

Mr. HYMAN. On the current implementation in Europe, there is an opt-out, do not share opportunity, beginning——

Senator COBURN. Every time?

Mr. HYMAN. Every time. As Mr. Wolf pointed out, certain devices because technologically do not support that, it is not available on every device. It is available through the computer on every device, and you can unshare afterwards. But the implementation that we have made is you start the movie, the presumption is sharing, and there is a "do not share" button that you can click afterwards, right when the movie starts. Anytime you deal with the movie, you can elect to not share. And then after the movie is displayed on Facebook, you can go back and adjust your setting within Netflix to unshare that. There are also sharings that you can do in the Facebook side.

Senator COBURN. So here is my question: What is the difference between an unshare opt-out and a share opt-out? They are both asking the same question. One is a presumption you are going to share all the time, but you are still making a decision each movie, unshare or not unshare.

Mr. HYMAN. Well, one is opt in and one is opt out.

Senator COBURN. Yes, but the point is the decision for privacy is still made individually on every movie that they send down the stream. So what is the difference of having an opt-in or an opt-out? It defeats your whole argument. They have the same thing.

Mr. WOLF. It does not defeat my argument, because I do not think it should be a matter of law.

Mr. HYMAN. I was going to say, I was going to echo—that is our implementation. Under the H.R. 2471, that is not required under law.

Senator COBURN. I understand that.

Mr. HYMAN. We have done that because that is what we believe consumers want. I think the issue for us at the highest level is really an informed consent. I think most everyone on this panel agrees, I think, philosophically on making sure that consumers understand what information they are disclosing or how their information is being handled. So at the high level, I think we are all coming to it from the same approach. I think there is a philosophical difference that in some way you highlighted on: Is it opt in, is it opt out, or is it—you know, how does Congress control the way in which consumers can share, are available to share? The presumption that we are trying to advocate for in connection with supporting H.R. 2471 is that it is really within the consumer's con-

trol to elect to do that if they so desire. It is an opt-in mechanism, and it is one in which they should be able to get informed consent.

I think there is a question on this panel of whether or not consumers can ever give informed consent. On our side, I think we would take the position that, yes, consumers can give informed consent. And, in fact, under the legislation there is a specific opt-out so that it is not buried in some terms of use, which we are in support of. So the issue about——

Senator COBURN. But if privacy is so important and if everybody at the table supports that, what is wrong with having the reminder that you are sharing your privacy? If it is that much of a value, if personal property rights and privacy rights are that important, what is wrong with having a reminder that you are giving away your privacy rights? If it is a value to be protected, if it is a virtue to be protected, your privacy, then what is wrong with the government saying there should be a reminder that you are giving your privacy away? What is wrong with that?

Mr. WOLF. There ought to be reminders, and government ought to support education of consumers through cyber education of kids to tell them what harm they might do themselves online by sharing TMI. But the number of reminders one would need every day would be in the thousands——

Senator COBURN. I do not need any reminders because I do not share anything.

[Laughter.]

Mr. WOLF. You are sharing your ideas right here, Senator.

Senator COBURN. But the point is I have to, under the ethics law, fill out forms at the end of every year, and I have to get that. As a part of participating in the Senate, there are certain things I have to do as part of my responsibility. But the point is, if privacy is of that value and you value that privacy and the protection of that privacy, what is wrong with us saying you need to have a reminder, to me, the Chairman, a 12-year-old, that you need to have a prompt to say you are giving away your privacy?

Mr. WOLF. So I can imagine someone opening up their mobile phone and they are about to talk in a public place and there is a law in Congress that says a pop-up has to appear that says, "You are in a public place. This is a reminder that you may be revealing private information about yourself. Click here to proceed."

Senator COBURN. You can imagine that. Again——

[Laughter.]

Mr. WOLF. Well, it is not so far away from what you are describing, Senator, because if we are going to require it for videos, there is no reason why we would not require it for all the other information that people choose to share. That is the world we live in. Certainly they should be given the right not to share, and they should be given the choice not to share. But I really do not think it is the job of Congress on such a granular basis to make that choice so difficult.

Senator COBURN. Well, what is difficult? They are having to pop the button now to say do not share. There is no difference. They are hitting the button share and unshare right now, so what is difficult about saying share versus unshare?

Mr. WOLF. I actually do not know what the experience has been in Europe with that and whether consumers object to it, whether they think it interferes with their experience or not.

Senator COBURN. He just testified that his consumers wanted that.

Mr. WOLF. I know it is available.

Mr. HYMAN. One issue, Senator, is that technology changes over time. So in order to implement that technology today, we are able to do it on certain devices. On other devices we are not able to do it. You know, and older legacy devices, we cannot go back and change those because of the way they have been designed. So, you know, people who have paid for some of our devices before now will not be able to take advantage of that feature because we cannot give them opt-out every time because Congress has told us we have to give them an opt-out every time?

I think the issue for us, again, is, you know, giving that control to the consumer, and if the consumer so elects to share on an ongoing basis, and perhaps even you could say to opt out of the notice to unshare, if they do not want to be bothered by it every time because that is inconvenient for them, they have chosen to give their movie watching onto Facebook or other social media platforms, should it be a law that they cannot do that? And I think from our perspective, it is very important that the consumers understand what they are doing and be given a choice. But to dictate exactly how that is implemented, especially in a dynamically changing environment in technology, I think it is important to be careful.

Senator COBURN. So what is wrong with what you just suggested, is you have an ability to opt out and then you have the ability to opt out of the opt-out question? What is wrong with that?

Mr. HYMAN. Fundamentally, I think that is fine, as long as you can get to the—you know, the way in which the process works, as long as——

Senator COBURN. Let me say it again. I am going to give you consent, Netflix, to share my movies. And then when a movie comes up, do you want to opt out? Or would you like to not see this screen again for six months and let all your sharing continue in your opt-in? In other words, for those that want to share everything, do not send me the reminder.

Mr. HYMAN. If that is what consumers want the way in which we would implement it, I am fine doing it. I have a little bit of trouble having that being legislated because I think over time that may change. It may be that six months is not the right amount of time. Is it three months? Is it a year? Is it never for certain people?

So in that sense, I think, from my perspective—I think the fundamental of taking a principle-based approach of consumers having control and consumers understanding what they are opting into or not opting into at their choice is the important thing that, you know, we as a people and you as legislators ought to focus on that fundamental.

And then the way in which it gets implemented, because things change over time, given technology, given the way people share and change, that should be somewhat left to being implemented.

Senator COBURN. OK, great point. Thank you, Mr. Chairman. Sorry I went over.

Senator FRANKEN. Not at all. I thought that was a very good line of questioning. I think it brought out a lot of great things, and we may not go to a second round because I was afraid that the Ranking Member would not be able to get enough time if he only got one round. But the Ranking Member went into a lot of great points, started early with an alcoholic husband who is afraid of his wife. I thought that was a good point. You might have a hangover and watch something his wife does not approve of. I thought that was a very good point.

That is a joke. I was kidding.

[Laughter.]

Senator FRANKEN. I think——

Senator COBURN. I am just not old enough to appreciate your humor.

Senator FRANKEN. No, I do not think it is that. I think that was probably—I think that joke curved foul.

[Laughter.]

Senator FRANKEN. But I think we do not need another round, but I think we—unless anyone wants to respond to a couple of observations I have here, because I think, Mr. Hyman, you said that it would not be buried in the terms of agreement, the ability to opt out. We do not know that. This piece of legislation does not say at all how opting out would work.

Mr. HYMAN. Actually, in 2471, there is a specific provision that was added in an amendment that said the actual agreement to share has to be separate and distinct from other legal and financial terms.

Senator FRANKEN. Yes, but not to opt out of the agreement.

Mr. HYMAN. Correct. The opt-out is not.

Senator FRANKEN. So that is the point. And you said that that would not be buried in the terms of agreement, and you talked yourself about how this is voluntary, and you were uncomfortable with that being in the law. This is voluntary because Netflix does what you do in Europe, but no other company would have to do it.

So I think that you underscore the point that the Ranking Member was making, which is it could be incredibly difficult to find out how to opt out of this once you have agreed—once you are sharing everything. I see Professor McGeveran nodding his head. I wonder if you have any thoughts on that.

Mr. MCGEVERAN. I am just agreeing. The Nadler amendment that was passed in the House bill does set up some specific requirements for how the original blanket consent has to be effectuated, but the bill is silent about what will be required to withdraw that consent later on if you decided you did not want a particular movie to be shared with your friends or that you wanted to cancel the previous authorization. It just does not say anything at all about how that would happen.

Senator FRANKEN. Right, and, you know, I think that, again, Netflix in Europe, where it can, on the devices where it works, gives people a clearer way to do that, but less scrupulous companies under the law would not be required to do that, and you would have to go through the terms and conditions, which can be pages and pages long, which none of us except for Professor McGeveran actually read.

Mr. WOLF. I read them, too, Senator.

Senator FRANKEN. OK, but they are privacy lawyers. Come on. No one reads those things. And I think that we almost got to the point of absurdity when—of course, you know, you do not have to be reminded that when you talk on your phone in public, we are not going to make it a law that, you know, someone could overhear you. And to reach for that kind of underscores, I think, sort of the common sense of if it is just as easy to click one button that says, "I want to share," you know, "watch and share," as opposed to "watch," it is no more burdensome to share each time on a one-by-one basis, as the original law claims, as opposed to having a consumer of a movie basically agree to sharing and then not be able to find where to opt out of that because it is buried in some place in the terms of agreement. No one has disputed that that is not written—that that is in the law to dictate that you can find it.

So I want to work with the Ranking Member on this because I think he really got to the gist of this, which is that we have to find—when you mentioned 30 days or 60 days or six months or something like that, I think maybe you could find a thing where someone says, "You know what? For the next 30 days, just share everything I like, and then remind me in 30 days," or something like that. I mean, I just think that this was kind of rushed through the Hous, maybe, and that we need to work on this——

Senator COBURN. I am happy to work with you.

Senator FRANKEN. Great. OK. So I am going to adjourn, and I know I am—I do not chair that much, so let me find—the record will be held open for a week.

[Laughter.]

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follows.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century"

Tuesday, January 31, 2012
Dirksen Senate Office Building, Room 226
10:00 a.m.

Panel I

The Honorable Melvin L. Watt
United States Congressman
State of North Carolina

Panel II

David Hyman
General Counsel
Netflix, Inc.
Los Gatos, CA

William McGeveran
Professor
University of Minnesota Law School
Minneapolis, MN

Marc Rotenberg
Executive Director
Electronic Privacy Information Center
Washington, DC

Christopher Wolf
Director, Privacy and Information Management Group
Hogan Lovells LLP
Washington, DC

PREPARED STATEMENT OF HON. PATRICK J. LEAHY

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Subcommittee On Privacy, Technology And The Law Hearing On
"The Video Privacy Protection Act: Protecting Viewer Privacy In The 21st Century"
January 31, 2012

I thank Senator Franken for the responsible leadership he is demonstrating as he chairs this panel on privacy. The right to privacy is one of our most fundamental freedoms. In his dissenting opinion in *Olmstead v. U.S.*, Justice Brandeis wrote that the Founders in our Constitution "*sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men.*"

In the digital age ensuring the right to privacy is crucial. But, protecting privacy has become ever more difficult, as our Government and businesses collect, store, mine and use our most sensitive personal information for their own purposes. Whether sensitive medical records, private financial information or personal thoughts and feelings, I have worked to ensure that Americans' privacy rights are respected.

In 1988, Congress enacted the Video Privacy Protection Act. When I first introduced the bill, I said that it was intended to help make all of us a little freer to watch what we choose, without public scrutiny. At that time, video rentals took the form of VHS tape rentals from local stores. We had just seen the publication of Supreme Court nominee Robert Bork's video viewing records and joined together to enact this statutory protection for the privacy of all Americans. My original proposal was also to include library records, but we were unable to sustain that protection as the bill worked its way through Congress. More recently, I have worked to add protections for library and bookseller records to section 215 of the USA PATRIOT Act.

While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the "cloud," mobile apps and other new technologies have revolutionized the availability of Americans' information. These new technologies are outpacing our privacy laws. That is why I continue to push to enact the Personal Data Privacy and Security Act, to create a nationwide data breach notification standard and better combat cybercrime, and it is why last year I proposed a comprehensive review and update of the Electronic Communications Privacy Act. I introduced a bill last May to update ECPA by requiring that the Government obtain a search warrant to access email content, or certain geolocation information. I have worked closely with Senator Franken on this issue, who has himself introduced legislation on location information.

Last week, I was encouraged by the Supreme Court's decision in the *Jones* case. That case discussed Americans' reasonable expectations of privacy in an era of vast technological change. It also dealt with how we think about and enforce the Constitution's guarantee against unreasonable search and seizure, a key aspect of our privacy rights. I believe that Congress needs to do its part to shore up Americans' constitutional right to privacy in an age of pervasive surveillance, with so much information available from, and collected by, service providers. While updating our Federal laws, we must carefully balance the need to promote American

innovation and the legitimate needs of law enforcement, while ensuring that we protect personal privacy.

Recently, companies that dominate various aspects of cyberspace have announced that they want to simplify matters so that they can more easily track Americans' activities across the board. I am not reassured by the prospect of "Big Brother" watching everything we do. I worry that sometimes what is "simpler" for corporate purposes is not better for consumers. It might be "simpler" for some if we had no privacy protections, no antitrust protections and no consumer protections, but that is not better for Americans. I worry about a loss of privacy because of the claimed benefit of "simplicity." This claim strikes me like the claim we often hear in large corporate merger proposals about so-called "efficiencies." Netflix announced a simpler billing practice a few months ago regarding its various services, and its customers rebelled.

Privacy advocates and elected representatives from both sides of the aisle have serious concerns and serious questions. We are asking for information and answers. When dominant corporate interests entice a check off in order to receive what may seem like a fun new app or service, they may not be presenting a realistic and informed choice to consumers. A one-time check off that has the effect of an all-time surrender of privacy does not seem to me the best course for consumers. I worry that the availability of vast stores of information via corporate databanks also makes this information readily available to the Government, which has almost unfettered power to obtain information with an administrative subpoena and so-called national security letters. These are issued unilaterally, without any judicial check or warrant requirement beforehand. That is why I think we need comprehensive reform to update our privacy laws.

I thank Representative Mel Watt, a thoughtful leader on these issues, for joining us, and the panel of witnesses assembled for sharing their views on this important subject. I am hearing from many privacy advocates who have expressed concerns about the privacy implications of the House-passed proposal. A key concern is that a one-time check off of consent to disclose, mine, sell and share information does not adequately protect the privacy of consumers. Nor does the House's proposal update the law with respect to streaming or cloud computing. We need to move forward with a comprehensive review and update of the Electronic Communications Privacy Act, and with it careful consideration of how best to update to the Video Privacy Protection Act.

#####

PREPARED STATEMENTS OF WITNESSES

Statement of Representative Melvin L. Watt (N.C. 12)

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century"

Tuesday, January 31, 2012
Dirksen Senate Office Building, Room 226
10:00 a.m.

Chairman Franken, Ranking Member Coburn and Members of the Subcommittee, I appreciate this opportunity to address the Subcommittee about the proposed amendment of the Video Privacy Protection Act ("the VPPA") and consumer privacy in this rapidly evolving digital age.

It is particularly timely that the Subcommittee holds this hearing today. Online privacy has been at the forefront of intense discussion for the past few years. Business leaders, consumer advocates, state and local elected representatives and officials from each branch of federal government have all weighed in with a variety of concerns and proposed solutions to address the absence of a uniform framework or approach to safeguard individual information in the thriving online environment. Attention has appropriately intensified as two of the Internet's giants—Facebook and Google—have come under scrutiny for their personal data usage policies and practices. Both Facebook and Google are currently subject to 20 year periodic audits of their privacy policies pursuant to separate settlements with the Federal Trade Commission (FTC)

entered into late last year.[1] Yet, just last week, Google announced sweeping changes to its privacy policy that users will not be allowed to "opt-out" of. The announcement has already raised the eyebrows of privacy advocates and could revive FTC probes into Google's practices.[2]

In the coming weeks, both the FTC[3] and the Department of Commerce[4] are expected to issue long anticipated final reports on online privacy policy based on a series of roundtable discussions with relevant stakeholders and following up on their initial studies in 2010.[5] Senators Kerry and McCain, in the Senate,[6] and Representative Cliff Stearns,[7] in the House, last year introduced comprehensive legislation designed to prescribe standards for the collection, storage, use, retention and dissemination of users' personally identifiable information. These bills also generated debate more generally in the Halls of Congress. This Subcommittee also held hearings to address the security of sensitive health records and personal privacy on mobile devices. And, last week, in deciding whether GPS tracking violates a criminal defendant's

---

[1] News Release, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," available at http://www.ftc.gov/opa/2011/11/privacysettlement.shtm; News Release, "FTC Gives Final Approval to Settlement with Google over Buzz Rollout," available at http://www.ftc.gov/opa/2011/10/buzz.shtm.

[2] Cecilia Kang, "Google announces privacy changes across products; users can't opt out," Jan. 24, 2012, Washington Post, available at http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html

[3] The FTC issued a preliminary staff report titled, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Business And Policymakers" in December 2010 following a series of stakeholder meetings. The report solicited comments and expected to issue a final report in 2011. The report is available here http://business.ftc.gov/privacy-and-security/consumer-privacy

[4] The Department of Commerce also issued a "green paper" in December 2010—"Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."

[5] *See* Abby Johnson, "Online Privacy Debate Heats Up With FTC And Commerce Dept. Reports Coming Soon," January 17, 2012 available at http://www.webpronews.com/online-privacy-debate-heats-up-with-ftc-and-commerce-dept-reports-coming-soon-2012-01.

[6] S.799, the Commercial Privacy Bill of Rights Act of 2011.

[7] H.R. 1528, the Consumer Privacy Protection Act of 2011.

Fourth Amendment right against unreasonable search and seizure[8], a majority of the Justices of the Supreme Court acknowledged the challenges we confront as a society in determining the "new normal" for privacy expectations in the digital age. In separate concurrences Justice Sotomayor, writing for herself, and Justice Alito, joined by Justices Ginsburg, Breyer and Kagan, pondered whether "[d]ramatic technological change may lead to periods in which popular expectations [of privacy] are in flux" and require the Court to rethink expectations of privacy where information is shared so freely.[9]

Although the Justices were deliberating expectations of privacy that give rise to a constitutional claim under the Fourth Amendment, that debate is not without significance in the context of this hearing today. Because of the inevitable disclosure of a wealth of personal information to third parties as a condition of using modern technologies, the intersection between commercial and constitutional privacy is palpable.[10] I believe that any legislative initiative in this realm must balance the right of individuals to privacy and control over their personal information, the interests of online commercial businesses in innovation and global competitiveness and legitimate law enforcement considerations.

Against this backdrop, I will direct the remainder of my comments to H.R. 2471, which passed in the House last session by a split vote of 303-116 under suspension of the rules. While I may not always avail myself of the new and revolutionary tools and services available over the

---

[8] U.S. v. Jones, 565 U.S. ___ (2012) (slip opinion).

[9] Id., (Alito, J., concurring in judgment), slip op. at 10.

[10] Justice Sotomayor observed that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks...Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" [online] of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not." Id., (Sotomayor, J., concurring), slip op. at 5 (citations omitted).

Internet, let me say at the outset that I fully appreciate and applaud the explosion of technological advances that has transformed forever the way we communicate and transact business. While I support innovation on the web, however, I cannot do so at the expense of individual privacy.

Given the gravity of the issues involved, I believe it was a mistake for this bill to move through the House relatively under the radar and without the benefit of a single hearing. But let me be clear: this is not just a process issue. I believe H.R. 2471 as passed will have unintended negative consequences for consumers and affected businesses, which will undoubtedly lose the confidence of their subscribers with the first privacy violation or data breach.

The history of the Video Privacy Protection Act, which is widely considered to be the strongest consumer privacy law in the United States, is well-known. The law was passed in 1988 following bipartisan outrage over the disclosure and publication of the video rental records of Supreme Court nominee Judge Robert Bork. Proponents of H.R. 2471argue that the VPPA is outdated and that changes in the commercial video distribution landscape justify modernization. Although the commercial distribution landscape has changed, the underlying concerns that inspired passage of the VPPA are timeless. Technology and privacy are not incompatible. We can and should promote technological innovation. But we must simultaneously prevent the unwarranted, uninformed disclosure of personal information for purposes over which the consumer invariably will lose control. Unfortunately, the amendment to the VPPA proposed in by H.R. 2471 chip away at those protections by equating technological expediency with consumer preferences. Consumer desire to have access to the next cool tool should not, however, be mistaken as the voluntary surrender of fundamental privacy interests. The

proliferation of privacy lawsuits and complaints against corporate giants like Google, Facebook, Apple and Netflix should make that imminently clear.

In addition to the lack of thoughtful process in the House, I believe there are at least four substantive problems with H.R. 2471. First, the bill leaves unaddressed the question of who the bill applies to, which I believe creates collateral, but important, intellectual property enforcement concerns. Second, although the debate on H.R. 2471 myopically centered on the online experience of consumers with social media like Facebook, the bill as passed applies to physical and online video tape service providers alike, and disclosures are authorized "to any person," not only "friends" on Facebook. Third, despite claims that the VPPA is "outdated," only a single provision of the statute was "updated," leaving consumer-oriented provisions that also should have been reviewed and strengthened unaltered. Fourth and finally, no consideration was given to the effect of the changes to the VPPA on state laws that afford similar and sometimes broader protections to consumers. Each of these concerns is discussed in greater detail below.

I. The definition of "video tape service provider" is left ambiguous by H.R. 2471

As Ranking Member of the Subcommittee on Intellectual Property, Competition, and the Internet of the House Judiciary Committee, I am concerned that in purportedly updating a statute to address new distribution models, H.R. 2471 failed to clarify who is covered by the Act. Under the VPPA, a "video tape service provider" is defined as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[11] When the VPPA was enacted, the primary method for the consumption of feature-length films by individual consumers was through the sale or rental of video cassette tapes. Today, consumers can assess video programming over a

[11] *See* 18 U.S.C. §2710 (a) (4) (2011).

variety of platforms including Internet Protocol Television, cable, or online streaming video-on-demand services.

In September 2011, Netflix[12] launched a public campaign in support of H.R. 2471, urging its subscribers to contact Congress to help bring Facebook sharing to Netflix USA.[13] Although Netflix is a legitimate and reputable company that provides a valuable service to its customers, its business model consists of a dual delivery method for movies and television which, I believe, complicates the application of the VPPA as narrowly amended to its distribution scheme. The company provides a mail order service for physical copies of DVDs and a streaming video-on-demand service to watch movies directly over the Internet. There is little doubt that Netflix's DVD by mail service is considered a videotape service provider under the statute. But neither the judiciary, regulatory body, nor Congress has concluded that Internet streaming services are covered by the statute.

The only court that has considered the issue summarily and without analysis rejected the argument that an online streaming service was prohibited (in an action alleging copyright infringement against the service), from producing its users' video history in discovery to enable the rights holder to determine whether the content was infringing.[14] Left unresolved is whether companies with dual distribution platforms (like Netflix) should be considered video tape service providers covered by the VPPA for social networking purposes and appropriately fall beyond the

[12] Founded in 1997, Netflix is the world's leading Internet subscription service. It provides movies and television shows through mail order DVD and online streaming services. With 900 employees, Netflix has 25 million subscribers worldwide. Netflix Company Facts, available at https://account.netflix.com/MediaCenter/Facts .

[13] Netflix has integrated user accounts in Canada and Latin America with Facebook, but advised its American customers that the VPPA "creates some confusion over our ability to let U.S. members automatically share the television shows and movies they watch with their friends on Facebook." Posting of Michael Drobac to The Netflix Blog, "Help us Bring Facebook Sharing to Netflix USA," (Sept. 22, 2011), http://blog.netflix.com/2011/09/help-us-bring-facebook-sharing-to.html.

[14] Viacom International, Inc. v. YouTube, Inc., No. 07 Civ. 2103 (S.D.N.Y., June 23, 2010).

statutes' reach for IP enforcement purposes or, alternatively whether streaming services will use the passage of H.R. 2471 to assert that Congress intended that the VPPA applies to both physical and virtual distribution methods. If the latter, I fear that online service providers will be able to have their cake and eat it too. In short, while enjoying the financial benefits of sharing its users' viewing history across platforms, a service provider could avoid or delay access to those same records in a meritorious copyright infringement dispute. By failing to address this fundamental issue, passage of H.R. 2471will add confusion rather than clarifying the law.

II. H.R. 2471 applies to all "video tape service providers" as defined by VPPA and disclosures are authorized to "any person."

In addition to failing to clarify what constitutes a "video tape service provider," H.R. 2471 leaves open the possibility that the very scenario that prompted passage of the VPPA could again expose consumers to unwanted disclosure and publication of their viewing histories.[15] Because H.R. 2471 focuses exclusively on a single disclosure requirement and does not address the VPPA as a whole, by its own terms the bill would apply to new and old distribution methods alike. There is nothing in the bill that would prevent a newspaper reporter from obtaining the rental or viewing history of a consumer who opts-in to the enduring, universal consent whether online or with a brick-and-mortar video store. In other words, nothing in the bill mandates that the disclosure be limited to social media integration. The bill simply gives carte blanche to video tape service providers, whether online or not, to disclose to "any person" a consumer's viewer

[15] Much has been made about the presumed disparity in treatment of video history as opposed to a consumer's reading lists or musical consumption habits. At the time the VPPA was enacted there were no comparable commercial music or book rental entities. The Committee Report did note, however, that the Senate subcommittee considered and "reported a restriction on the disclosure of library borrower records... [but] was unable to resolve questions regarding the application of such a provision for law enforcement." S. Rep. No. 100-599 (1988), at 8.

history provided they have obtained the "informed" consent of the consumer in a conspicuous manner.

My concerns are not eased, and indeed are exacerbated, when consent is sought in the online environment. At a time when the broader privacy debate is trending towards establishing some baseline privacy protections for consumers online, I believe this bill moves in the opposite direction. Although consumers can withdraw their consent at any time, I do not believe that option adequately reflects the realities of the instant, permanent, widespread dissemination and consumption of users' content.

Facebook—the largest social media network –boasts 800 million users, with the average user having 120 "friends." But because Facebook, and most social platforms, are dynamic with a user's roster of friends constantly in flux, a consumer's consent today to allow perpetual access to their viewing history is clearly not informed by who will be their "friend" tomorrow. Today when the online bullying of teen and young adults can lead to depression or even suicide and online predators can learn otherwise confidential, private information about their prey, I believe the selective, piecemeal "modernization" of the VPPA is simply irresponsible. "[M]ovie and rating data contains information of a more highly personal and sensitive nature. The member's movie data exposes a …member's personal interest and/or struggles with various highly personal issues, including sexuality, mental illness, recovery from alcoholism, and victimization from incest, physical abuse, domestic violence, adultery, and rape."[16] The VPPA established robust protections for precisely this type of information. Passage of H.R. 2471 would seriously compromise those robust protections.

III. Consumer oriented provisions of the VPPA are not "updated" by H.R. 2471.

[16] Ryan Singed, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims," WIRED, December 17, 2009, available at: http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit.

In the inexplicable rush to pass this bill, I believe important consumer protection issues were overlooked. The VPPA was enacted to protect consumer interests in personally identifiable records. Yet H.R. 2471 focuses singularly on facilitating disclosure, not preventing, limiting, or protecting that interest. The bill's exclusive aim is to provide a safe haven for wide-scale disclosures made possible by technological innovation. In the process, the goal of insulating personal information from unwanted disclosure is completely neglected. In fact, none of the consumer-oriented provisions of the underlying Act are amended to reflect modern day circumstances.

For example, the VPPA requires destruction of records "as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected." Record retention and destruction plans reinforce policies designed to deter the abuse or misuse of personally identifiable material. They generally set forth guidelines to those with access to an individuals' personal information that prohibit storing documents beyond their usefulness or discarding them prematurely. The rationale embodied in the provision in the VPPA that requires the destruction of video records no later than a year after the record was established was clearly driven by the desire to prevent stockpiling of old and outdated data on any person. True modernization of the VPPA should also have considered the feasibility and desirability of applying that same provision in the online environment.

Some internet companies have been found to track, retain, market and mine information on their customers at an alarmingly high rate.[17] Conventional wisdom teaches that once information is posted on or over the Internet, it remains stored or cached there forever. Thus, while record destruction in the physical world is more easily effected and verified, that is not the

[17] *See* "The Web's New Gold Mine: Your Secrets," WSJ Julia Angwin (July 30, 2010).

case in the virtual world. The question arises whether additional safeguards should be enacted to ensure that the policy objectives underlying the requirement in the VPPA to destroy old records are transferrable to the online environment.[18]

Additionally, while easing the restrictions on video service providers to disclose its users' video histories, H.R. 2471 ignores the damages provision for consumers harmed by violations of the VPPA. In 1988 when the VPPA was passed, Congress calculated that a minimum of $2,500 in actual damages was an adequate deterrent to discourage violations of the Act. Certainly that figure, although a floor, is outdated today where revenues earned by companies online can exceed billions of dollars and permanent disclosure of a consumer's intimate information can extend to much larger audiences.

IV. No consideration was given to the effect of the changes to the VPPA on state laws that afford similar protections to consumers.

According to the Electronic Privacy Information Center (EPIC), many states have laws that extend greater protections to consumers and their video records than does the VPPA. Among the states that have adopted comparable or stronger measures are: Connecticut, Maryland, California, Delaware, Iowa, Louisiana, New York, Rhode Island and Michigan. Michigan's law actually applies to book purchases, rental and borrowing records, as well as to video records. And California recently passed a law updating its reader privacy laws to apply to Electronic books.[19] The House did not evaluate what practical impact H.R. 2471 would have on those states laws. The VPPA expressly preserves state law that establishes more robust

[18] Netflix is currently in class action litigation over claims that the company's practice of keeping the rental history and ratings "long after subscribers cancel their Netflix subscription," violates the VPPA. http://www.huntonprivacyblog.com/2011/03/articles/netflix-sued-for-allegedly-violating-movie-renters-privacy/.

[19] *See* http://www.aclu-sc.org/releases/view/802934.

safeguards for consumers in their relationships with video rental services. The VPPA, however, preempts state law that requires disclosures otherwise banned by the VPPA.

Conclusion

During consideration of H.R. 2471 before the House Judiciary Committee I offered two amendments, both designed to give Internet businesses the necessary flexibility to obtain electronic consent from consumers, while simultaneously safeguarding privacy rights. While there may be other more precise and effective means to balance these objectives, I believe that H.R. 2471 is clearly not that alternative.

Mr. Chairman, this past Saturday was "Data Privacy Day."[20] Data Privacy Day recognizes the importance of educating consumers on how to preserve the security and privacy of their personal and potentially sensitive information shared over the Internet. While Internet users have a responsibility to self-censor and restrict the information they share about themselves, the reality is that many online users have a false sense of privacy due to a lack of understanding of lengthy and complex privacy policies to which they are compelled to agree in order to use the service. As a result, online users have a tendency to share a lot of personal information unknowingly and with unintended audiences. I do not believe that the unsuspecting, unsophisticated or casual Internet user should be deemed to relinquish his right to a basic level of privacy. As Justice Marshall wrote years ago, "Privacy is not a discrete commodity, possessed absolutely or not at all."[21] The trick is to strike an appropriate balance to develop meaningful protections for consumers while promoting a healthy online economy. I support a comprehensive online privacy plan that will address and mitigate the unintended consequences of third party sharing. In that regard, I believe

[20] Data Protection Day began in Europe in 2007. The following year, the United States and Canada initiated "Data Privacy Day" which is celebrated annually in late January/early February with participants from the U.S., Canada and over 40 countries in the Council of Europe. Events associated with Data Privacy Day are designed to reach and involve consumers and consumer advocates, businesses and government officials to promote awareness about developments in the intersection between data collection and privacy protection. *See* http://www.staysafeonline.org/dpd/about.

[21] Smith v. Maryland, 442 U.S. 735, 749 (1979).

Justice Alito got it right: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[22] This hearing is a responsible beginning to that effort and even more critically important because the House failed to give the matters the kind of attention required. I thank the Chairman for this opportunity and look forward to working across the Capitol moving forward.

[22] Jones, 565 U.S. ___, (Alito, J., concurring in judgment), slip op. at 5.

Written Testimony of David Hyman
General Counsel of Netflix, Inc.

Before a Hearing of

The Committee on the Judiciary of the U.S. Senate
Subcommittee on Privacy, Technology, and the Law

On

"The Video Privacy Protection Act:
Protecting Viewer Privacy in the 21st Century"

Tuesday, January 31, 2012

Chairman Franken, Ranking Member Coburn, and distinguished members of the Subcommittee. Thank you for the opportunity to testify today about the Video Privacy Protection Act.

My name is David Hyman. I have served as the General Counsel of Netflix since 2002: A time when streaming video over the Internet to a "smart" TV was more the stuff of a sci-fi mini-series than a topic of serious consideration in a corporate board room, much less a congressional hearing. How far we have come in such a short period of time. Today's hearing is a testament to the incredibly dynamic and powerful innovation engine of our Internet economy.

Netflix was founded in 1997 as a DVD-by-mail service. To many, the use of the Internet and the Netflix website was nothing more than a way to submit orders for physical disc delivery. But for Netflix, we saw an opportunity to use technology in a way that helped consumers discover movies and TV shows they would love, as well as provide business opportunities for content producers and distributors.

The popularity of our DVD-by-mail service grew rapidly. But with innovation deeply rooted in our corporate DNA, we continued to research and try new and compelling consumer offerings. We were an early pioneer in streaming movies & TV shows over the Internet to personal computers. In 2008, we began to deliver instant streaming video to televisions through the use of a handful of Internet-connected devices. Today, more than 21 million consumers in the United States use the Netflix streaming service on more than 700 different types of Internet-connected devices, including game consoles, mobile phones and tablets. And, in the last three months of 2011, we delivered more than 2 billion hours of streaming movies and TV shows to those consumers.

At the same time the Netflix streaming service has seen such uptake by consumers, the world of social media has exploded in popularity. Embodied by the growth of Facebook, the social Internet offers tremendous opportunities for consumers and businesses Netflix believes that social media offers a powerful new way for consumers to enjoy and discover movies and TV shows they will love. To this end, we have been offering our members outside the United States the opportunity to share and discover movies with their friends through the Facebook platform. While it's still early in the innovation process, we have seen strong consumer interest in our social application, with more than half a million subscribers outside the United States connected with Facebook.

Unfortunately, we have elected not to offer our Facebook application in the United States because of ambiguities in the Video Privacy Protection Act. Under this law, it is unclear whether consumers can give ongoing consent to allow Netflix to share the movies and TV shows they've instantly watched through our service. The VPPA is an unusual law; unlike most federal privacy statutes, the VPPA could be read to prohibit consumers who have provided explicit opt-in consent from being able to authorize the disclosure on an ongoing basis of information they so desire to share. The friction that this ambiguity creates places a drag on social video innovation that is not present in any other medium, including music, books, and even news stories.

Recognizing this, the House recently passed a bi-partisan bill, H.R. 2471, that clarifies consumers' ability to elect to share movies and TV shows they've watched on an ongoing basis. H.R. 2471 leaves the opt-in standard for privacy within the VPPA undisturbed. Netflix supports an opt-in regime for movie title sharing and believes this approach is workable and consistent with our members' expectations and desires.

The VPPA singles out one type of data sharing. Instead of trying to graft specific notions about video privacy from almost 25 years ago into the dynamic information age of today, we would encourage a measured and holistic review of privacy for the 21st century, one designed to foster continued innovation while balancing the desires and privacy expectations of consumers. Such a review will understandably take considerable time and effort and we are ready to assist. In the interim, it is our hope that the Senate will see the value in clarifying the right of consumers to opt-in to ongoing sharing under the VPPA and quickly approve H.R. 2471.

Again, thank you for the opportunity to appear before you today, and I look forward to your questions.

Testimony of William McGeveran
Associate Professor, University of Minnesota Law School

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
The Video Privacy Protection Act in the 21st Century
January 31, 2012

Thank you to Chairman Franken, Senator Coburn, and the entire subcommittee and its staff for the opportunity to speak to you about this legislation.

My name is William McGeveran. I am a law professor at the University of Minnesota. My teaching and research focus on internet, data privacy, and intellectual property law. In that context I have written about the Video Privacy Protection Act, which I consider a model for privacy legislation more generally. I am also a member of the Advisory Board of the Future of Privacy Forum.

Unquestionably there are great benefits to the online recommendations we get from friends through sources like Facebook or Spotify – I myself use social media heavily. But the potential problems are serious too. In one article I argued that the key to getting that balance right is securing ***genuine consent***.[1] That means an individual sent a social message intentionally, not by mistake. If we have too many accidental disclosures, we undermine the privacy of personal matters and the accuracy of the recommendations. The VPPA is designed to secure genuine consent.

In this testimony I want to emphasize three principal points:

- First, the VPPA safeguards important interests.
- Second, changes are not needed to keep up with technology.
- Finally, even if Congress does amend the statute, H.R. 2471 does it wrong.

1. "Intellectual privacy" is an important principle that Congress should expand, not constrict

First, the VPPA safeguards important interests. The movies we watch can reveal personal characteristics, from our sexuality to our political views to our medical conditions. Why else did a newspaper reporter think Judge Bork's rental history might be interesting in the first place?

---

[1] William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, available at http://illinoislawreview.org/article/disclosure-endorsement-and-identity-in-social-marketing/.

Unintended disclosure of a user's choice of books, music, films, or web sites can constrain the capacity to experiment and to explore ideas freely. For this reason, we intuitively recognize the interest underlying the VPPA – as well as confidentiality protections for library patrons' records, for example. Data privacy scholar Neil Richards calls this "intellectual privacy."[2] It recognizes the fundamental First Amendment value inherent in leaving individuals alone as they gain exposure to a wide variety of ideas, without necessarily labeling themselves.

In my view, the greatest flaw in the existing VPPA is its limitation to video, which arises from a historical accident around its enactment. If the committee revisits this statute, it should consider extending protection to reading and listening habits as well as viewing. That was part of the intent of the California Reader Protection Act, which took effect at the beginning of the month.[3] In general, the law ought to protect ***private*** access to any work covered by copyright, not just movies.[4]

2. The VPPA Is Flexible and Already Enables Online and Social Media Implementations

Second, the VPPA, ***in its current form***, already allows video companies to implement social media strategies such as integrating with Facebook. There has been commentary suggesting this law is some musty and outdated relic, but that simply is not true.

Now, it ***is*** true that the VPPA requires opt-in consent every time a viewer's movie choices get forwarded to a third party, including a friend in a social network. Blockbuster's original implementation of the disastrous Facebook Beacon initiative failed to do this, and it probably violated the VPPA as a result.[5]

But it's actually ***easier*** to satisfy those requirements online than off. The statute's authors envisioned a video rental store getting the customer to sign a

---

[2] *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); *see also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1003–19 (1996).

[3] S.B. 602 (Cal. 2011), http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0601-0650/sb_602_bill_20111002_chaptered.pdf.

[4] *See generally, e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002); Richards, supra note 2; American Library Association, Code of Ethics, available at http://www.ala.org/advocacy/proethics/codeofethics/codeethics.

[5] *See* James Grimmelmann, *Facebook and the VPPA: Uh-Oh*, THE LABORATORIUM (Dec. 10, 2007), http://laboratorium.net/archive/2007/12/10/facebook_and_the_vppa_uhoh; William McGeveran, *Beacon Lawsuit Faces Uphill Climb*, INFO/LAW (Sept. 15, 2008), http://blogs.law.harvard.edu/infolaw/2008/09/15/beacon-lawsuit-analysis/.

separate document, in person, for every disclosure. On the internet, by comparison, each time users push the button to play a movie, they could get a "play and share" button right alongside it allowing them to post that information in social networks as well.

I have always agreed with the bill's supporters that different users have different desires about the amount of information they reveal, and that good privacy law allows people to control their own degree of disclosure.[6] The concept of genuine consent gives precisely that control to the user. Constant intrusive pop-up windows asking for permission are not desirable. But the interface I describe above is nothing of the sort. Since the user must take an affirmative act to play the video, I am at a loss to understand how pairing it with privacy consent presents any difficulty.

Some have suggested that the VPPA's "written consent" provision might require pen and paper rather than such online authorization.[7] I disagree. That interpretation would undermine every clickwrap and "I agree" button on the internet. It is contrary to the E-SIGN Act[8] and to all the caselaw I've seen.[9]

A typical user's social networking profile is loaded with personal information, but most of it is there precisely because the user made an affirmative opt-in choice to post it. Status updates, location check-ins, and photos do not ordinarily pop onto your Facebook page without your explicit case-by-case permission. The VPPA-compliant structure described above would make sharing of videos quite similar.

A world with too much passive sharing in social networks places all of us in fishbowls where our intellectual and entertainment choices face scrutiny. Passive sharing inevitably causes accidental disclosures. Where intellectual privacy is at stake, these disclosures can be harmful, and the VPPA does and should protect the individual. Intentional disclosures are great opportunities for

---

[6] I so argue in my very first publication about privacy, a law review note. William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1837-38 (2001).

[7] See, e.g., Jules Polonetsky and Christopher Wolf, *Viewers Should Be Able to Share Their Playlists*, ROLL CALL (Nov. 29, 2011).

[8] 15 U.S.C. §§ 7001-7031.

[9] See, e.g., Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 556 (1st Cir. 2005) (holding that E-SIGN Act "likely precludes any flat rule that a contract to arbitrate is unenforceable under the ADA solely because its promulgator chose to use e-mail as the medium to effectuate the agreement"); Berry v. Webloyalty.com, Inc., 2011 WL 1375665 at *7 (S.D. Cal. April 11, 2011) (granting Rule 12(b)(6) motion to dismiss claim because E-SIGN Act means that clicking "yes" button satisfied written consent requirement in another federal statute).

us to recommend to one another great songs (or movies, or newspaper articles) and the VPPA encourages these interactions.

Netflix may wish to integrate with Faceboook using the same structure as Spotify or the Washington Post's Social Reader app. The fact that the VPPA does not allow this structure reflects its demand of genuine consent.

The real objection of the bill's sponsors is not about technology. It's a disagreement with the VPPA's policy choice to get case-by-case consent rather than a one-time authorization. The only reason for Congress to change this law is to weaken its privacy protections.

3. If Congress does amend the VPPA, it needs to fix many problems in H.R. 2471.

Finally, H.R. 2471 has a lot of problems, and it misses some opportunities for reasonable compromise.

First, the problems. To begin with, even though social networking was the impetus for this bill, it is vital to remember the alterations of the VPPA made in H.R. 2471 apply across the board to all disclosures by all video services. By rushing to address Netflix and Facebook, the bill reduces privacy in many settings, from law enforcement to behavioral advertising.

To the extent that Congress decides to make changes inspired by social networking – and I have argued for skepticism about doing so – this would be better accomplished with a particular exception from the VPPA. A tailored social media exception would respond better to the particular concerns Netflix and other bill supporters have raised, without distorting the remainder of the VPPA.

That said, it is important to remember that intellectual privacy interests don't diminish when the disclosures go to our friends and contacts through social media – they ***increase***. That's partly because many "friends" in social networks are half-forgotten high school classmates. But as to true friends and close family, those may be exactly the people who will make judgments about our movie queues. Ask yourself whether you would be more uncomfortable showing your entire movie-watching history to your mother or to a faceless advertising company.

In sum, H.R. 2471 unravels the entire consent structure of the VPPA merely to address a perceived shortcoming in social networking disclosures.

Second, by specifically mentioning the internet, H.R. 2471 may ***foreclose*** electronic consent through other technologies such as cable or satellite. The version of H.R. 2471 passed by the House describes consent as "written consent (including through an electronic means using the Internet)." This text could be read to ***limit*** the VPPA's application of the E-SIGN Act to only those electronic

communications "using the internet," potentially foreclosing current and future technology that bypasses the internet. For example, mobile devices such as the Kindle or satellite radio that might show movies could be forbidden from getting written consent electronically – exactly the opposite of the sponsors' intent. So, too, might the interfaces of cable television companies' on-demand or DVR services. I imagine this was not the drafter's purpose, but it demonstrates the unintended consequences that arise when writing a bill with one particular scenario in mind. It would be better for the bill to remain silent on the issue and rely on the E-SIGN Act's default rule, to refer to the E-SIGN Act, or to repeat its language.

Third, although H.R. 2471 contemplates permanent one-time blanket consent, it also allows a customer to "withdraw" that consent at a later time. Unfortunately, there is no guidance about the nature of this revocation and it may lead to serious complexity and difficulties. For starters, the withdrawal presumably could not be retroactive and would have no effect on disclosures already made. More significantly, there is no indication of ***how*** the customer would revoke consent, and no obligation on the video services provider to explain it to the customer. This lack of specificity in H.R. 2471 will create headaches all around. On one side, since there is no requirement that a withdrawal be written, could an oral request to a telephone customer service representative count as a binding withdrawal, imposing potential liability on the provider for any subsequent disclosures? Conversely, could companies comply with the statute after it was amended by H.R 2471 by making it easy to give consent but difficult to revoke it? It seems that under the bill a video provider might not offer any convenient online mechanism to withdraw consent, or might even specifically require such customers to send a written request to a postal address. These scenarios may seem unlikely, and certainly would be undesirable, but nothing in H.R. 2471 specifies how that process ought to work.

Even more important than these problems are the opportunities unaddressed by the narrow approach of H.R. 2471. If Congress chooses to amend the VPPA, I urge you to do so in a more comprehensive fashion than this bill, which appears to be crafted only to advance one company's business plan rather than to reexamine the VPPA.

Some of the language in the statute could be modernized and made more precise. For example, the statute should update the terminology around "video tape service providers." Even though the VPPA's definition explicitly embraces providers of "similar audio visual materials,"[10] the dated language could mislead a judge into thinking that new technology such as streaming falls outside the VPPA's scope. Simply deleting the word "tape" would ensure that the particular physical medium remains irrelevant, as the VPPA's authors clearly intended.

---

[10] 18 U.S.C. § 2710(a)(4).

Most significantly, however, H.R. 2471 replaces the robust consent provisions of the VPPA with a very weak alternative. Even as amended by Congressman Nadler in the House of Representatives, the bill allows an unclear request for authorization when a customer signs up – likely worded to encourage agreement – and does nothing to regulate the customer's subsequent modification of permission. This arrangement fails to secure genuine consent.

That said, I certainly do not believe that the model of the VPPA is the ***only*** route to genuine consent. There may be other creative ways. For instance, what about general authorization with a short time limit (say, one month) and granular, clear opt-out for all individual posts? The lack of a hearing on the bill in the House prevented proper exploration of such ideas. Several members of the House committee attempted to explore middle-ground alternatives, but unfortunately the rushed markup process did not allow time for the emergence of carefully considered consent procedures.

In conclusion, the VPPA is a model privacy bill advancing important interests in intellectual privacy. New technology actually makes it easier, not more difficult, to comply with the statute's requirement for case-by-case authorization for disclosures. If the Senate nonetheless pursues a bill to amend the VPPA, I urge the committee and the bill's supporters to seek creative compromises that might update the VPPA for the 21st century without vitiating its protection for individuals' intellectual privacy.

I would be happy to work with you further as the legislative process for this bill continues.

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on
"The Video Privacy Protection Act:
Protecting Viewer Privacy in the 21st Century"

Before the

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

January 31, 2012
226 Dirksen Senate Office Building
Washington, DC

Introduction

Mister Chairman and Members of the Subcommittee, thank you for the opportunity to testify today concerning the "Video Privacy Protection Act and Protecting Viewer Privacy in the 21st Century." My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center ("EPIC"), and I teach information privacy law at Georgetown University Law Center.

EPIC is non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy. EPIC has a particular interest in promoting technical standards and legal safeguards that help safeguard personal information.[1]

We thank you for holding the hearing today and for taking the time to consider the important issue of online privacy.

Summary

In my statement today I will explain EPIC's interest in this legislation, describe the history and purpose of the Act, underscore the concerns that users today have about online privacy, and emphasize the importance of protecting the privacy going forward. I will urge the Committee to reject the approach taken by the House in H.R. 2471, which does little more than gut one of the key safeguards in the law. Instead, I will ask you to consider several amendments that would in fact update and modernize the law.

The Video Privacy Protection Act was a carefully crafted privacy law that addressed competing concerns, while setting out principles that were technology neutral and forward-looking. Some amendments to the law would be appropriate, but they should strengthen not undermine the rights of users. Changes to the law should also respond to the reality that companies today collect far more personal information about their customers than companies did twenty-five years ago when the law was adopted. That point alone argues in favor of strengthening the statute.

EPIC's Interest in Video Privacy

EPIC has a strong interest in supporting the rights of Internet users to control the disclosure of their data held by private companies. We have specifically worked to protect the privacy rights for consumers that were established by the Video Privacy Protection Act.

In 2009, EPIC filed an *amicus curiae* brief supporting strong privacy safeguards for consumers' video rental data.[2] EPIC's brief urged the Fifth Circuit Court of Appeals to enforce

[1] More information about EPIC is available at the web site http://www.epic.org/.
[2] *Harris v. Blockbuster*, No. 09-10420 (5th Cir. Nov. 3, 2009) *available at* http://epic.org/amicus/blockbuster/Blockbuster_amicus.pdf.

the law's protections for Facebook users who rented videos from Blockbuster, a Facebook business partner. Facebook users filed the lawsuit after Blockbuster made public consumers' private video rental information.

In 2010, EPIC wrote to the U.S. District Court for the Northern District of California, urging the court to reject a proposed settlement that would have deprived Facebook users of remedies under the video privacy law.[3] EPIC urged the Court to reject a settlement that would have resulted in no direct compensation for users, despite the law's $2,500 statutory damages provision. EPIC also observed that the settlement would have deprived users of meaningful privacy protections by directing all settlement funds to a Facebook-controlled entity.

EPIC has also opposed the recent effort to undermine the Video Privacy law.[4] In our letter to House members last year on H.R. 2471 we urged careful consideration of the impact that the proposed change would have on users of Internet-based services. At a minimum, we asked the Committees considering the legislation to hold a hearing so that that all views on the matter could be considered. Unfortunately, the House pushed through the change without any hearing, without any real opportunity to hear competing views.

The Importance of Internet Privacy

There is no issue of greater concern to Internet users today than protecting the privacy and security of personal information. Polls reveal that users are concerned about the privacy of their personal information online, with 88 percent of parents supporting laws requiring companies to obtain opt-in consent before collecting and using personal information.[5] For eleven years, the Federal Trade Commission's has found that identity theft is the top source of consumer complaints.[6]

These concerns are well-founded. Last year, many high-profile companies, such as Citigroup,[7] Bank of America,[8] and Sony[9] lost consumer data in their possession as a result of data breaches.

---

[3] EPIC, "Letter from the Electronic Privacy Information Center to The Honorable Richard G. Seeborg re: *Lane v. Facebook*, proposed settlement" (Jan. 15, 2010) *available at* http://epic.org/privacy/facebook/EPIC_Beacon_Letter.pdf.

[4] EPIC, "Letter from the Electronic Privacy Information Center to Congressman Mel Watt re: Proposed Amendments to the Video Privacy Protection Act" (Dec. 5, 2011) *available at* http://epic.org/privacy/vppa/EPIC-on-HR-2471-VPPA.pdf.

[5] Diane Bartz and Gary Hill, *Parents, teens want more privacy online: poll*, REUTERS (Oct. 8, 2010), http://www.reuters.com/article/2010/10/08/us-privacy-poll-idUSTRE69751820101008.

[6] Press Release, Federal Trade Commission, TC Releases List of Top Consumer Complaints in 2010; Identity Theft Tops the List Again (Mar. 8, 2011), http://ftc.gov/opa/2011/03/topcomplaints.shtm.

[7] Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. Times (June 16, 2011), http://www.nytimes.com/2011/06/16/technology/16citi.html?_r=1.

[8] David Lazarus, *Bank of America Data Leak Destroys Trust*, L.A. Times (May 24, 2011), http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524

In fact, Netflix has already been at the center of one of these privacy breaches. In 2006, Netflix published 10 million movie rankings given by 500,000 customers, whose names were replaced by random numbers. The company claimed that there would be no risk to the privacy of their users. But researchers were able to use publicly available information to reidentify many of these users, revealing customer's video viewing history over a given period of time.[10] The breach prompted a class-action lawsuit, which Netflix eventually settled.[11]

More recently, Netflix was sued for violating the Video Privacy law by retaining records of users rental and viewing habits after users had deleted their accounts.[12] The law wisely anticipated that retaining user data after it was needed would expose consumers to unnecessary risk. And many companies today routinely adopt the principle of "data minimization." But – instead of complying with the requirement that the collection of user data be limited, Netflix began its effort to overturn the Video Privacy law, arguing among other points that the damages provision was unconstitutional.[13]

The debate over online privacy and Netflix does not exist in a vacuum. It is becoming increasingly clear that only privacy laws actually safeguard the privacy rights of Internet users.

The Federal Trade Commission had made some progress in protecting the privacy of consumers' information as a result of complaints brought by EPIC and other consumer and civil liberties organizations. The FTC announced settlements with both Google and Facebook.[14] The settlements prohibit the companies from misrepresenting the privacy and security protections on personal information, and require the companies to obtain the affirmative consent of users before disclosing personal information to a third party in a way that exceeds users' current privacy settings.[15]

---

[9] Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive data breach*, Reuters (April 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[10] *See* Bruce Schneier, *Why "Anonymous" Data Sometimes Isn't*, WIRED (Dec. 13, 2007), http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213; *see also* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf.

[11] Natalie Newman, *Netflix Sued for "Largest Voluntary Privacy Breach To Date"*, PROSAKAUER PRIVACY LAW BLOG (Dec. 28, 2009), http://privacylaw.proskauer.com/2009/12/articles/invasion-of-privacy/netflix-sued-for-largest-voluntary-privacy-breach-to-date/.

[12] Christophor Rick, *Netflix To Attack Privacy Law As Unconstitutional, Raises Further Privacy Issues*, REELSEO http://www.reelseo.com/netflix-privacy-law/#ixzz1kgoxuvfn (last visited Jan. 31, 2012).

[13] *Id.*

[14] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm; Press Release, Federal Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm.

[15] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order), http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.; see also Google, Inc., FTC File No. 102 3136 (2011) (Decision and Order) http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

Despite the recent FTC settlements, Google and Facebook continue to change their business practices in ways that lessen the ability of users to control their information. For example, Facebook launched Timeline, which made personal information that users thought had "vanished" suddenly available online.[16] Users had to go back through their postings to remove wall posts that might be inappropriate or embarrassing.

And Google announced that it would begin combining user data across 60 separate Google services.[17] Google did not give users the option to opt-out while continuing to use Google's services. So the only option for a user who had expected that Google would not link information about the location of her Android smartphone with information about the content of her Gmail messages is to stop using both services. Members of Congress[18] and federal agencies[19] have raised concerns over how this data consolidation would affect consumers and federal employees.

Under pressure from the GSA, it appears that Google has backed off its proposed changes for services offered to the federal government because of obvious concerns about taking information provided by federal employees for email services and making it available to Google for other services. But so far Google has not backed off plans to consolidate user data outside of its contracts with the federal government.

The lesson of the recent episodes with the Federal Trade Commission settlements, and the subsequent action by the companies is that it may be only federal privacy laws, such as the Video Privacy Protection Act, that provide meaningful privacy protections to Internet users.

The Video Privacy Protection Act Establishes Meaningful Safeguards for Consumers' Video Rental Records

At the time of the Video Privacy Protection Act's enactment, lawmakers recognized the substantial privacy risks posed by collection, retention, and disclosure of video rental records. These risks were demonstrated when Judge Robert Bork's video rental records were published, without his consent, during hearings concerning the Judge Bork's nomination to the U.S. Supreme Court.[20] The Washington City Paper published analysis of Judge Bork's video rentals

---

[16] F8 DEVELOPERS CONFERENCE 2011, https://f8.facebook.com/ (last visited Jan. 31, 2012).
[17] *Updating our privacy policies and terms of service*, THE OFFICIAL GOOGLE BLOG (Jan. 24, 2012), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.
[18] Letter from Cliff Stearns, et al., to Larry Page, CEO, Google Inc., (Jan. 26, 2012), http://democrats.energycommerce.house.gov/sites/default/files/documents/Page.Google.2012.1.26.pdf.
[19] Alice Lipowicz, *Google's new privacy policy raises new worries for feds*, FEDERAL COMPUTER WEEK (Jan. 25, 2012), http://fcw.com/articles/2012/01/25/googles-new-privacy-policy-could-have-impacts-on-feds-at-work-and-at-home.aspx.
[20] Michael Dolan, *The Bork Tapes*, Washington City Paper, Sept. 25-Oct. 1, 1987 *available at* http://www.theamericanporch.com/bork5.htm.

on its front page, writing "Never mind his writings on *Roe vs. Wade*. The inner workings of Robert Bork's mind are revealed by the videos he rents."[21]

Although there was a sharp disagreement among Committee members about the nomination of Judge Bork, there was no disagreement about the importance of establishing a new privacy law to protect the consumers of video services that were increasingly moving from the broadcast environment of television and movies to a digital world where companies can record detailed information about their customers.

In several respects, the Video Privacy Protection Act is a model privacy law. It is technology neutral and focuses on the collection and use of personal information. The aim is to protect personal information, not to regulate technology. The presumption is in favor of privacy, but there is no flat prohibition. The law creates narrow exceptions that permit disclosure in certain well-defined circumstances. For example, the Video Privacy Law permits disclosure to law enforcement agencies pursuant to a warrant, grand jury subpoena, or court order.[22] Additionally, the law permits disclosure pursuant to a court order during civil discovery. [23] And of course, the consumer retains the right to consent to the disclosure of her personal data.[24]

Regarding the use of personal data for marketing purposes, there was a compromise struck. Marketers were free to disclose general information about their customers under an opt-out standard. But where a company wanted to disclose the title of the actual movies viewed, the company was required to get meaningful consent on a case-by-case basis. It is that critical provision, which safeguard the privacy of users, that Netflix now wants to undo.

The Video Privacy Protection Act did not go as far as it might have gone in light of technology and business models that have emerged since the law's enactment. Companies collect far more data today than they did before and consumers are at greater risk today of identity theft and security breaches than they were when the law was adopted.

The Proposed Amendment Would Undermine Consumers' Privacy Rights

To answer the concerns that Netflix has expressed, the Video Privacy Protection Act does not prevent Netflix from integrating its services with Facebook. It does not prevent Netflix from disclosing that a Facebook user is using Netflix or even the genre of film that the viewer is watching. In fact, the Video Privacy law even permits Netflix to disclose on Facebook the name of the movie a viewer is watching *as long as the user meaningfully consents.*

---

[21] *Id*; *see also* Cover Image, http://www.theamericanporch.com/new_stuff/IMG_8988c.jpg.
[22] The Video Privacy Protection Act, Pub. L 100-618, codified at 18 U.S.C. § 2710 (b) (2) (C).
[23] Id. § 2710(b) (2) (F).
[24] Id. § 2710(b) (2) (B).

Although Netflix argues that obtaining consumer consent to disclose information each time a consumer watches a video is cumbersome, in the absence of an alternative, it is still the most effective way to obtain meaningful consent. Consumers acquiescing to a one-time blanket consent to cover future video choices is not meaningful consent. Consumers likely do not plan movie choices months in advance, and likely will not recall that their consent to share their innocuous children's movie selection will also apply to their more provocative selections.

The proposed amendment replaces the Video Privacy law's carefully crafted consent requirements with a blanket consent provision. The amendment would transfer control from individuals to the company in possession of the consumer's data and diminish the control that Netflix customers have in the use and disclosure of their personal information.

Under the current statute, Netflix and Facebook are required to obtain user consent at the time "the disclosure is sought."[25] Under the proposed amendment, companies such as Netflix and Facebook could obtain consent once, and subsequently disclose hundreds or thousands of movie selections linked with personally identifiable information for years or decades to come. Companies could also make the blanket consent provision a condition of using their services, thereby removing all meaningful consent and effectively eviscerating the Act.[26] Either approach would gut the Video Privacy Law.

While we recognize that other social network companies routinely report on the activities of their customers, we note that Facebook users have never been particularly happy about this. Take for example, Facebook's "Beacon." The now defunct Facebook advertising tool would broadcast—without user consent— a user's interaction with an advertiser to the feeds of that user's friends. As with Beacon's disclosure of online viewing history, routine disclosure of video viewing activities is not something that most Facebook users are clamoring for. Viewer consent should therefore be given on a case-by-case basis, which reflects the intent of the drafters of the Act.

We should also note that the implicit endorsement that Netflix is seeking to elicit from the users of its services might also be false and misleading. Imagine if Netflix made a point of routinely posting the movies that Netflix's customers are viewing and someone in fact concluded that the movie they were viewing was really not very good and certainly not one that they would recommend that their friends view. Netflix would nonetheless be advertising to that person's friends and to others that the person is viewing the movie with the implicit message that they too might want to subscribe to Netflix so they can view the movie as well.

---

[25] The Video Privacy Protection Act, Pub. L 100-618, codified at 18 U.S.C. § 2710 (b)(2)(B).

[26] Certain popular digital music services, such as Spotify, have already made social media integration mandatory. Paul Sawers, *New Spotify users are now required to have a Facebook account*, THE NEXT WEB, Sept. 26, 2011, http://thenextweb.com/facebook/2011/09/26/new-spotify-users-are-now-required-to-have-a-facebook-account/. Because disclosing data associated with digital music services is unregulated, companies like Spotify can force social media integration by removing meaningful consent. Amending the VPPA to permit one-time blanket consent could permit video tape service providers to adhere to the digital music service business model at the expense of consumer privacy.

That can't be right.

Congress Should Modernize the Video Privacy Law to Protect the Interests of Users

Congress should indeed update the video privacy law, but it should do so in a way that strengthens the law. The current bill would amend the video privacy law by removing a core privacy protection – the requirement that companies obtain consumers' consent before each disclosure of personal information. Thus, the amendment would transfer control over disclosure of video records from the consumer to the company.

Rather than enact the proposed amendment, EPIC recommends that Congress amend the Video Privacy Protection Act to strengthen the Act's protections. Congress should amend the Video Privacy Law to: (1) make clear that the law applies to all companies offering video services; (2) create a right of access and correction for consumers; (3) explicitly recognize that Internet Protocol (IP) addresses and user account numbers are personal information; (4) strengthen the Act's damages provision; and (5) require companies to encrypt consumers' personal information. These changes are necessary in light of new business practices and the privacy concerns of consumers.

(1) Congress Should Make Clear that the Video Privacy Law Applies to All Companies Offering Video Services

As adopted in 1988, the term "video tape service provider" was intended to be comprehensive. The Act defines the term to include providers of "prerecorded video cassette tapes or similar audio visual materials."[27] Despite the drafters' clear intent, some Internet video service providers have argued that the companies' video rentals are not subject to the Act. Congress should amend to Video Privacy law to make clear that the Act applies to all video service providers.

We would propose an amendment that clarifies that the law applies to all videotape service providers. The law currently states:

> (4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

We would propose the addition of a new provision to resolve the ambiguity.

---

[27] 18 U.S.C. § 2710(a)(4).

(5) the term "similar audio visual materials" in subsection (a)(4) means audio visual materials in any format delivered by any means, including but not limited to digital audio visual materials delivered *via* streaming or download.

(2) Congress Should Create a Right of Access and Correction for Consumers

The Video Privacy law allows a video service providers to disclose an individual's rental history at the consumer's request. But the Act does not provide consumers with a right to access this information nor to examine the algorithm, or "logic," that is used to make recommendations for that consumer.

The right of access is a crucial tool that helps consumers understand what personal information companies collect and retain, and how it is used. Several privacy statutes include provisions that assure individuals the right to access their personal information.[28] Moreover, access to the algorithm will help users better understand how recommendations are made.

We propose a right of access to the data of the consumer and the logic of the processing be adopted in the Video Privacy Protection Act by adding the following language in paragraph 2710(b)(2):

If a consumer requests access to information under subparagraph (A) of subsection (b)(2), a video tape service provider shall clearly and accurately disclose the requested information, including the logic of the processing of the consumer's data, to the consumer. The video tape service provider shall make such disclosure within twenty-four hours of receiving the request.

(3) Congress Should Explicitly Recognize that Internet Protocol (IP) Addresses and Account Identifiers are Personal Information Covered by the Act

The Video Privacy law defines the term "personally identifiable information" ("PII") as data that can link consumers to their video rental history. The Act is intended to be broadly construed, covering all information that is linked or can be linked to a renter. However, because Internet-based video distribution did not exist in 1988, the Act does not explicitly include Internet Protocol (IP) Addresses in the definition.

IP addresses can be used to identify users and link consumers to digital video rentals. They are akin to Internet versions of consumers' home telephone numbers. Every computer connected to the Internet receives an IP address that is logged by web servers as the user browses the Internet. These logs allow companies to record a trail of the user's online activity. Companies engage in extensive tracking and data collection about the online activities on consumers.[29]

---

[28] *E.g.* Fair Credit Reporting Act of 1970, Pub. L. 91-508, codified at 15 U.S.C. § 1681; The Privacy Act of 1974, Pub. L. 93-579, codified at 5 U.S.C. § 552a.

[29] *See, e.g.*, Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, at A1; *see also* Jessica E. Vascellaro, *Google Agonizes on Privacy as Ad World Vaults Ahead*, WALL ST. J., Aug. 10, 2010, at A1.

Furthermore, user names, which are frequently disclosed in URLs, can be used to personally identify users.[30]

We would propose the addition of Internet Protocol (IP) Addresses and account identifiers to the definition of PII as follows:

> (3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider[begin insert], including but not limited to Internet Protocol (IP) addresses and account identifiers; and

(4) Congress Should Inflation-Adjust the Act's Damages Provision

The Video Privacy Protection Act includes a liquidated damages provision in an amount of $2,500. This was an appropriate amount when the Act was adopted in 1988. However, over time, the value of this award has diminished in real terms. Increasing the liquidated damages amount to $5,000, taking into account inflation over the past twenty-five years, would restore the damage provision that Congress intended be in place when the Act was adopted.

We propose the following change:

> (c) Civil action.--(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.
> (2) The court may award--
> (A) actual damages but not less than liquidated damages in an amount of ~~$2,500~~$5,000

(5) Congress Should Require Companies to Encrypt Consumers' Personal Information

The Video Privacy law was enacted before video rental records were routinely stored in digital form. Indeed, Judge Bork's video rental list – the list that publicized the insecurity of American's rental histories – was kept on paper.

Today, the vast majority of video rental records are stored in computer databases. Computerized records are uniquely susceptible to wrongful access, as illustrated by many recent, high-profile data breaches affecting companies like Sony,[31] Citigroup,[32] and Wells Fargo.[33] Common-sense use of encryption reduces this risk.

---

[30] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, STANFORD CENTER FOR INTERNET & SOC'Y (Oct. 11, 2011 8:06am), http://cyberlaw.stanford.edu/node/6740.
[31] Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive data breach*, Reuters (April 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.
[32] Dan Goodin, *Citigroup Hit With* Another *Data Leak,* The Register, Aug. 9, 2011, http://www.theregister.co.uk/2011/08/09/citigroup_data_breach_again/.
[33] The Associated Press, *Wells Fargo Data Breach Revealed*, L. A. Times (August 13, 2008), http://articles.latimes.com/2008/aug/13/business/fi-wells13.

We would propose that the law be amended to require encryption of personal information as follows:

> (g) A person subject to this section shall employ reasonable security practices to protect a consumer's personally identifiable information. Failure to encrypt personally identifiable information is an unreasonable security practice.

Congress Needs to Pass Meaningful Privacy Legislation

I would also like to take the opportunity of this hearing to suggest that the Senate should move forward important privacy legislation to safeguard Internet users and consumers of new Internet-based services.

Several bills have been introduced in the Senate that would make important contributions to the protection of privacy. For example, the Data Privacy Bill of 2011, which is aimed at increasing protection for Americans' personal information and privacy. [34] The bill establishes a national breach notification standard, and requires businesses to safeguard consumer information and allow consumers to correct inaccurate information.

The Location Privacy Protection Act would place requirements on the collection and use of consumers' location data by companies. [35] And the Personal Data and Breach Accountability Act would protect the personal information of consumers by requiring businesses to implement personal data privacy and security programs. [36]

As the problems with the Google and Facebook FTC settlements make clear, meaningful legislation is the best way to protect consumer privacy.

Conclusion

The Video Privacy Protection Act was a smart forward-looking privacy law that focused on the collection and use of personal information by companies offering new video services. It was technology neutral, setting out rights and responsibilities associated with the collection and use of personal data that applied regardless of the method employed to deliver video services. The proposed amendment does not update the law, it simply undermines meaningful consent. However, the bill could be usefully updated and modernized by incorporating the changes we have proposed. Those changes would help protect the interests of Internet users. And it is of course their data that is at issue.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

---

[34] S. __ (2011), http://www.leahy.senate.gov/imo/media/doc/BillText-PersonalDataPrivacyAndSecurityAct.pdf.
[35] S. 1223.
[36] S. 1535.

REFERENCES

EPIC, "Video Privacy Protection Act"
http://epic.org/privacy/vppa/

EPIC, "Letter from the Electronic Privacy Information Center to Congressman Mel Watt re: Proposed Amendments to the Video Privacy Protection Act" (Dec. 5, 2011)
http://epic.org/privacy/vppa/EPIC-on-HR-2471-VPPA.pdf

United States Senate

Committee on the Judiciary

Testimony before the Subcommittee on Privacy, Technology and the Law

"The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century"

January 31, 2012

Christopher Wolf
Director, Privacy and Information Management Practice, Hogan Lovells US LLP
Founder and Co-Chair, Future of Privacy Forum

Chairman Franken, Ranking Member Coburn, and distinguished members of the Subcommittee. Thank you for the opportunity to testify about video viewer privacy.

Background

My name is Christopher Wolf and I am a privacy lawyer at Hogan Lovells US LLP, where I lead that firm's global privacy practice. I also am the founder and co-chair of the Future of Privacy Forum, a think tank with an Advisory Board from business, consumer advocacy and academia, focused on practical ways to advance privacy.

I have been a privacy law practitioner since virtually the start of the discipline, and I have long been a privacy advocate. One of my earliest privacy law matters was representing *pro bono* a gay sailor about whom the Navy illegally obtained information from AOL in violation of the Electronic Communications Privacy Act in order to oust him under the Don't Ask, Don't Tell law then in effect. The Navy's conduct was declared illegal by a federal judge and the Navy quickly recognized the wrongdoing. That case and others demonstrated to me the perils of personal information being shared without permission.

Through my law practice, I have broad exposure to privacy issues. I regularly represent clients before the Federal Trade Commission on privacy matters, in litigation, in corporate transactions and for compliance counseling. I produced a comprehensive treatise on privacy law for the Practising Law Institute, in addition to other published writings on the subject, and have taught law school courses on Internet law and privacy. I am a member of a volunteer panel of experts that advises the OECD Working Party on Information Security and Privacy and I am on the Advisory Board of the Electronic Privacy Information Center.

I participate in the major discussions of the day concerning the future of privacy. I have presented at the annual International Conference of Data Protection and Privacy Commissioners; I was the only privacy lawyer to speak at the eG8 Forum preceding the 2011 meeting of the G8 in France; I am a regular participant in the Privacy Law Scholars Conference and other academic conferences; I am a regular presenter at programs of the International Association of Privacy Professionals; I maintain a privacy law blog; and this week I am one of four organizer/moderators (along with three privacy law professors) at the annual Privacy Law Salon, a two-day gathering of privacy leaders.

I am pleased to offer my perspectives as a privacy law practitioner, as a participant in policy discussions on the future of privacy and as an advocate of improved privacy protections for video viewers in the 21st century.

Privacy is a Matter of Personal Control and the Pre-Internet VPPA Limits Personal Control to the Extent it Restricts a Durable Sharing Option

In considering how best to protect viewer privacy, it is important to understand that privacy is not the same thing as secrecy. Privacy is about *control*. Indeed, a goal of privacy law and the Fair Information Practice Principles underlying it is to put decisions in the hands of informed consumers.[1]

The Video Privacy Protection (VPPA), enacted nearly a quarter of a century ago, was designed to prevent prying into people's video rental history, an issue brought to light through the infamous incident involving a newspaper reporter obtaining video records about Judge Robert Bork at the time he was under consideration for the Supreme Court.

The purpose of the VPPA was *not* to stop people from sharing information about the videos they watched or to stop companies from using that data if consumers consented. Instead, the VPPA's purpose was to put the *control* in the hands of consumers, to let the consumers decide whether to share their video-watching information.

Since the VPPA's passage, technology rapidly has advanced to allow people to watch movies through streaming video services instead of going to a video store, but the privacy law for video rentals hasn't changed in over two decades. The VPPA was passed at a time when streaming video and social network sharing were not remotely contemplated.

So when that pre-Internet-era law is applied to the world of online video and social media, it can be read to frustrate the choice of consumers who want to authorize the disclosure on an ongoing basis of the streaming movies they watch online.[2] Facebook users commonly utilize a one-time authorization – a durable choice option – to share a wide range of information with their friends. But their ability to use such an authorization to share video-watching experiences arguably is thwarted by the restrictive, outdated language of the statute requiring "consent of the consumer given at the time the disclosure is sought."[3]

In the Facebook era, regular sharing of information with friends is routine, accepted and embraced.[4] People share the music they listen to, the books and newspaper articles they read, the meetings and

---

[1] The Fair Information Practice Principles are notice, choice, access, security, and enforcement.
[2] Under the statute, "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person," 18 U.S.C. § 2710(b)(1), and "the term 'video tape service provider' means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes *or similar audio visual materials*." *Id.* § 2710(a)(4) (emphasis supplied). "A video tape service provider may disclose personally identifiable information concerning any consumer . . . to any person with the informed, written consent of the *consumer given at the time the disclosure is sought*." *Id.* § 2710(b)(2)(B) (emphasis supplied).
[3] *Id.*
[4] *See* Don Reisinger, *Spotify paying subscribers jumps to 2.5 million*, CNET (Nov. 23, 2011), *available at* http://news.cnet.com/8301-13506_3-57330417-17/spotify-paying-subscribers-jumps-to-2.5-million. Mathew Ingram, *Why Facebook's Frictionless Sharing Is the Future*, BLOOMBERG BUSINESSWEEK (Oct. 3, 2011), *available at* http://www.businessweek.com/technology/why-facebooks-frictionless-sharing-is-the-future-10032011.html.

lectures they attend, the trips they take and so on. But under the VPPA, it can be said that web users cannot share the videos they watch in the same way. This makes no sense.

Imagine a person who is an avid online video watcher, watching 100 short videos per week. She wants to share every video that she watches with her friends, just as she shares every song she listens to on the streaming music service Spotify and just as she shares every item she reads online on the Washington Post through its Facebook social sharing app. But current law inconsistently suggests that she is not fit to make this frictionless sharing decision with respect to the videos she watches. Should this videophile have to opt in 100 times per week? Does making her do so serve any purpose other than to really annoy her and take needless time? The law as embodied in the VPPA can be read to take control away from this hypothetical video fan and dictate how she can share in the social media world.

By contrast, there are no legal restrictions on her ability to socially share every book she downloads onto an e-book reader. This gives rise to the inconsistent result that disclosure from a one-time opt-in that she viewed the movie *The Girl with the Dragon Tattoo* is legally suspect, while a similar disclosure that she read the book *The Girl with the Dragon Tattoo* is perfectly fine.

I am not aware of any other situation where consumers are prevented from opting in to ongoing sharing of their information and are required to consent to disclosures on a per-transaction basis. Even in the European Union, which has the strictest privacy standards in the world, one-time consent is necessary and sufficient to place cookies for the purpose of online behavioral advertising.[5]

Unless the VPPA is amended to specifically allow easier sharing through a durable choice option, which some people do want, the VPPA stands as an obstacle to the free flow of information and to consumer choice, without providing a commensurate privacy benefit in return.

Those Who Don't Want to Share Won't Have to Even if the Durable Sharing Choice is Allowed

Of course, not everyone wants to share their viewing experiences with their friends online, and they don't have to share. And if web users prefer to share their video-watching experiences on a case-by-case basis, they can do so manually, just as people occasionally post news stories they read in the Washington Post on Facebook rather than downloading the app that automatically shares this information. Similarly, a person who chooses to share on a continuous basis can disable the share function before watching a streaming video that he or she wants to exclude from online posting. That addresses one of the primary arguments advanced to oppose amendment of the VPPA: that with the amendment, a user automatically and inadvertently may post a recent viewing experience that allows others to draw unwanted conclusions about that person's religious, political or social viewpoints. But that argument presupposes that web users can't exercise that readily available choice for themselves.

The key to protecting privacy is not to be paternalistic and deny people the right to share information as they wish or to assume they don't know what they are doing online.

---

[5] *See, e.g.*, ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 16/2011 ON EASA/IAB BEST PRACTICE RECOMMENDATION ON ONLINE BEHAVIOURAL ADVERTISING 10, 02005/11/EN, WP 188 (Dec. 8, 2011) ("[O]nce a user has expressed his/her consent or refusal then there is no need to ask him/her again for consent for a cookie serving the same purpose and originating from the same provider.").

A good privacy law makes it easy for people to do what they want – either to share or not share. Good privacy regulation makes sure that consumers are informed about their choices and the consequences, but ultimately leaves the decisions in the hands of consumers.

Privacy law is not designed to inhibit information flow, but to empower consumers to control information flow. Amending the VPPA to allow people to have durable choice concerning their sharing preferences will modernize the law to reflect the advent of technology and social media, and to be consistent with the Fair Information Practice Principles. Such an amendment will reflect a proper balance between privacy and the innovative free flow of information. I join the Center for Democracy and Technology in concluding that the proposed amendment to permit the durable choice option does not "undermine[] the fundamental purpose of the law."[6]

The Durable Sharing Choice Should Be Opt-In and Prominent

To be clear, I favor opt-in as the choice mechanism for ongoing sharing of video viewing under the VPPA rather than an opt-out arrangement where sharing is the default unless the consumer objects. And the opt-in choice mechanism should be prominent, separate and distinct from a site's general privacy policy and terms of service, as required by the House amendment to the VPPA, H.R. 2471.

Opt-in consent represents the strongest level of choice available in U.S. privacy laws. Thus, with opt-in as the standard, consumers should have the option of saying: "I want to share my video information now and into the future until such time as I change my mind." If consumers opt in and later decide that they don't want to share, they simply can withdraw their consent. The VPPA currently does not allow this. Instead, it appears to require consumers to keep opting in, over and over again.

The Other Risks of Not Permitting the Durable Sharing Choice

Indeed, requiring users to choose to share their video-viewing habits on a per-video basis (for example, by requiring users to check another box before sharing can occur) inappropriately elevates the privacy of online videos over the privacy of other information for which the law does *not* require repeated choices. Or, quite possibly, it may lead to the situation where consumers feel inundated by privacy choices to the point that they are numbed by and pay no attention to them, merely clicking through to get on with the online experience.

And with respect to the impact on business, Congress did not intend to pick winners and losers when it passed the VPPA, but the law does exactly that, unintentionally, because it can be read to handicap streaming video companies from taking advantage of social media tools while other media companies can provide their customers with a social media sharing tool.

Permitting the Durable Sharing Choice Consistent with the Evolution of Privacy Law

We are at a consequential time in the development of privacy law, here and abroad. The European Union is considering dramatic revisions to its privacy framework[7] while the Obama Administration

[6] Center for Democracy and Technology, *House Tweaks Video Privacy Law for Frictionless Sharing* (Dec. 7, 2011), http://www.cdt.org/blogs/justin-brookman/712house-tweaks-video-privacy-law-frictionless-sharing.

[7] European Commission, Press Release, *Commission proposes a comprehensive reform of the data protection rules* (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

and the Federal Trade Commission are about to unveil their proposals for a new approach to privacy protection, which have been previewed extensively through drafts.

One clear trend is observable in the movement towards reform and improvement of privacy law around the world, and that is an avoidance of piecemeal, technology-specific rules, what I frequently refer to as a "patchwork quilt" of regulation.

Instead, baseline privacy protections that are technology-neutral represent the modern approach to privacy law. This is a framework that consumers can understand and that businesses can implement easily. Accordingly, an integral component of privacy law reform is revising or repealing laws from the old framework in order to achieve consistency. Amendment of the VPPA to permit full user choice and control fits squarely within the preferred framework.

Thank you for the opportunity to appear before you today.

QUESTIONS FOR WILLIAM MCGEVERAN SUBMITTED BY SENATOR AL FRANKEN

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century"
January 31, 2012

Questions for the Record from U.S. Senator Al Franken
for Professor Bill McGeveran

1. **The Video Privacy Protection Act ensures that when a video provider no longer needs information about you, that information must be destroyed. The less data there is about you, the less likely misuse is. And not just misuse by commercial entities, but also misuse by the government. As the *Tin Drum* case demonstrates, government misuse of video viewing data is very possible.**

   My understanding is that there is currently a difference of opinion between federal courts as to whether or not individuals can enforce the VPPA's data destruction requirement via the private right of action. Can you explain why that requirement is important, and why we need to make sure it is enforceable?

QUESTIONS FOR MARC ROTENBERG SUBMITTED BY SENATOR AL FRANKEN

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century"
January 31, 2012

Questions for the Record from U.S. Senator Al Franken
for Mr. Marc Rotenberg

1. **The Video Privacy Protection Act protects more than just consumer privacy—it protects our civil liberties as well. The American Civil Liberties Union wrote me a letter, which has been entered into the official record, talking about the importance of maintaining privacy in the things we watch. This letter also raises serious concerns about the effects of H.R. 2471 on civil liberties.**

   Could you explain the civil liberties protections the Video Privacy Protection Act provides, and how H.R. 2471 might affect those protections?

2. **In comments filed in the House, Representative Watt pointed out that if H.R. 2471 passes, it wouldn't just affect Netflix and Facebook. It would affect all video companies, online or offline, reputable or not. And in doing so, it would allow easier sharing with a lot of people who aren't your friends, on Facebook or off of Facebook.**

   What could H.R. 2471 mean for customers of brick and mortar video stores or online video companies that aren't as reputable as Netflix?

QUESTIONS FOR DAVID HYMAN SUBMITTED BY SENATOR TOM COBURN

Written Questions of Senator Tom Coburn, M.D.
David Hyman
General Counsel, Netflix, Inc.
U.S. Senate Committee on the Judiciary
February 7, 2012

1. Do you believe your consumers benefit when Netflix integrates with social networks in countries outside of the United States? If so, how?

    a. What prompted Netflix to develop this sharing app in other countries?

    b. What has been the consumer response in other countries to Netflix's sharing app?

2. In your testimony, you asserted it would be good policy for Congress to amend the Video Privacy Protection Act (VPPA) to permit consumers to provide on-going consent to share their viewing histories. Why do you believe this is good policy?

    a. Why do you believe allowing consumers to give on-going consent, in this context, is preferable to giving consent each and every time?

    b. What are the technical difficulties, if any, with providing consumers with the option of whether to share each and every time they view a movie or TV show?

    c. Do companies providing other types of media such as music or books permit a one-time opt-in for customers?

    d. What would be the difference, if any, between allowing consumers to opt-in to sharing everything for a set period of time as opposed to choosing not to be asked whether they want to share each and every time for a set period of time (a sort of opt-out, opt-out option)?

    e. If Congress decided to amend the VPPA to permit customers to opt-in on a continuous basis for a set period of time, what period of time would be reasonable in your mind - three months, six months, a year or some other period of time?

3. In your testimony, you stated that as a consumer-driven company, Netflix would always provide consumers with an easy method for withdrawing their consent because that is what consumers want. H.R. 2471 requires opt-in consent to be "informed, written consent ... in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer..." However, this legislation does not specify if a company must provide a clear opt-out option. If Congress were to amend the House legislation, would you support language that would ensure bad actors are not able to make withdrawal of consent difficult for consumers?

4. In the countries where Netflix already offers their sharing service, can consumers use Netflix's other services without using the application that shares their viewing histories on Facebook or another social network?

5. Should Congress extend the VPPA to cover other "streaming" services or types of media? Why or why not?

6. Concerns have been raised that passing H.R. 2471 would allow video tape service providers to disclose the movie and TV titles a video renter has watched to any third party of the video tape service provider's choosing. What, if anything, would prevent video tape service providers from doing this?

    a. If the VPPA is amended in a manner consistent with H.R. 2471, could a consumer unknowingly or inadvertently consent to allowing a video tape service provider to sell information about the movie and TV titles that consumer has watched? Why or why not?

    b. Does current law prevent this?

7. Concerns have been raised that allowing on-going consent could result in consumers accidentally disclosing movie or TV titles to friends or family that a consumer might not actually wish to disclose. Does the Netflix app have any safeguards in place to prevent this?

QUESTIONS FOR CHRISTOPHER WOLF SUBMITTED BY SENATOR TOM COBURN

Written Questions of Senator Tom Coburn, M.D.
Christopher Wolf
Director, Privacy and Information Management Group, Hogan Lovells LLP
U.S. Senate Committee on the Judiciary
February 7, 2012

1. In your testimony, you asserted it would be good policy for Congress to amend the Video Privacy Protection Act (VPPA) to permit consumers to provide on-going consent to share their viewing histories. Why do you believe this is good policy?

    a. Why do you believe allowing consumers to give on-going consent is preferable to giving consent each and every time?

    b. Do companies providing other types of media such as music or books permit a one-time opt-in for customers?

    c. What would be the difference, if any, between allowing consumers to opt-in to sharing everything for a set period of time as opposed to choosing not to be asked whether they want to share each and every time for a set period of time (a sort of opt-out, opt-out option)?

2. Would every Netflix customer have to use an application that shares their viewing histories on Facebook or another social network if Netflix was able to offer this service in the U.S.?

3. Should Congress extend the VPPA to cover other "streaming" services or types of media? Why or why not?

4. Concerns have been raised that passing H.R. 2471 would allow video tape service providers to disclose the movie and TV titles a video renter has watched to any third party of the video tape service provider's choosing. What, if anything, would prevent video tape service providers from doing this?

    a. If the VPPA is amended in a manner consistent with H.R. 2471, could a consumer unknowingly or inadvertently consent to allowing a video tape service provider to sell information about the movie and TV titles that consumer has watched? Why or why not?

    b. Does current law prevent this?

    c. Does anything prevent the same concern being raised with other sharing apps such as for book or movies?

5. Is is easy for customers to discontinue using other sharing apps such as Spotify and Washington Post Social Reader?

    a. To your knowledge, have there been any customer complaints regarding the difficulty of opting out or terminating service with any of these sharing apps?

QUESTIONS AND ANSWERS

NOTE: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from William McGeveran.

NOTE: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from Marc Rotenberg.

RESPONSES OF DAVID HYMAN TO QUESTIONS SUBMITTED BY SENATOR TOM COBURN

NETFLIX

RESPONSE TO QUESTIONS FOR THE RECORD FROM SENATOR TOM COBURN, M.D.

Submitted By: David Hyman, General Counsel, Netflix, Inc.

March 6, 2012

1. **Do you believe your consumers benefit when Netflix integrates with social networks in countries outside of the United States? If so, how?**

The popularity and use of social networks has grown significantly over the past several years. By integrating our service with social networks, we provide our consumers with the opportunity to leverage the power of their social networks with their content viewing. Our consumers are able to benefit from a richer video watching experience by sharing the content they have watched with their own community of friends, similar to what they can currently do with the music sharing service Spotify. In doing so, our consumers benefit from a new way to engage in dialogue around the content they are watching. Enhancing Netflix by making it more social increases the chances that members will discover movies and TV shows they will love. In this way, social media is the new water cooler around which folks enjoy and share their movie and TV show watching experience. The more readily consumers are able to discover great content, the richer the cultural experience consumers enjoy.

Enabling more robust discovery of movie and TV shows also benefits other participants in the entertainment ecosystem, particularly those individuals who are associated with movies and TV shows that may not have received broad scale promotion or distribution. Independent producers and all the writers, directors and craftspeople that produce this kind of entertainment welcome additional ways to get their content out for viewing. Social integration makes discovering interesting, independent, foreign, or library content easier for consumers, which in turn benefits the creators of that content. Netflix already provides a boost to such content by helping surface it through our recommendation algorithm and user interfaces. Our integration with social media provides yet another vehicle for content discovery, augmenting benefits to our consumers and those that produce such content.

a. What prompted Netflix to develop this sharing app in other countries?

Social media and sharing is a worldwide phenomenon. We wanted to develop our sharing application here in the U.S., but ambiguities in the VPPA prevented us from doing so. We see social video as an important and growing component of our consumers' content viewing experience. We developed our social application (excluding the U.S.) because it is something our consumers want and offering it provides them with a great way to share and enhance their content viewing experience.

b. What has been the consumer response in other countries to Netflix's sharing app?

Over half a million of our international subscribers have opted-in to our social application. In fact, reviews in the UK and Latin America of our service comparing it to other content distribution services have noted our social functionality as a positive competitive differentiator.

2. In your testimony, you asserted it would be good policy for Congress to amend the Video Privacy Protection Act (VPPA) to permit consumers to provide on-going consent to share their viewing histories. Why do you believe this is good policy?

Social media has and continues to rapidly change the way in which we interact with each other and share our daily experiences with our family and friends. The growth and popularity of services like Facebook, Groupon, Zynga, LinkedIn, and Spotify exemplify this trend. Consumers who want to participate in this growing phenomenon and, in a knowing manner, decide to share things they are doing on an ongoing basis, should not be prevented by law from doing so. During oral testimony, several persuasive arguments were made to demonstrate that, while some people may choose not to engage in such a level of sharing, the law should not prohibit individuals who decide to opt-in. Additionally, from a policy perspective, the VPPA is an outlier in privacy law. By singling out video tape service providers, this law treats one type of media, video cassette tapes or similar materials, differently than books, music, and news articles. Such disparate treatment does not seem to have a sound basis in public policy.

a. Why do you believe allowing consumers to give on-going consent, in this context, is preferable to giving consent each and every time?

First, as indicated above, we do not believe the United States Congress should prohibit an individual from electing to engage in ongoing sharing if such individual affirmatively elects to do so. Second, enabling frictionless sharing on social networks is consistent with consumer preferences. Legally forcing a consumer to give consent every time diminishes that consumer's ability to efficiently express

himself with friends and family. The Internet is designed to promote just such efficiency, and social media has harnessed new and exciting ways to do so for consumers. Furthermore, simply because a law permits a consumer to share in an ongoing manner, does not require a consumer to do so. Consumers will always have the option of sharing on social networks on a title-by-title basis by manually doing the sharing themselves. If there is no privacy benefit to prohibiting ongoing consent, but there is diminished enjoyment of a service due to enforced title-by-title consent, then the preferable policy should be one that permits consumers to give ongoing consent.

b. What are the technical difficulties, if any, with providing consumers with the option of whether to share each and every time they view a movie or TV show?

The complication with a title-by-title consent regime as applied to the Netflix service is primarily related to devices. We offer our service on over 700 devices and not all of those devices can be updated in a way that would enable a consumer to make granular choices about sharing. Technological realities limit compliance with per-title sharing requirements.

As new technologies develop, laws that prescribe certain behavior tend to become impediments to effective innovation, because these laws do not properly anticipate future changes. The law should encourage innovation while balancing the interests of consumers by focusing on principles-based rules. Requiring opt-in consent for emerging technologies such as social media sharing will fully protect consumer expectations in this new environment.

3. Do companies providing other types of media such as music or books permit a one-time opt-in for customers?

Yes. Companies such as Spotify, Rdio, Yahoo!News, and others provide one-time opt-in for consumers.

a. What would be the difference, if any, between allowing consumers to opt-in to sharing everything for a set period of time as opposed to choosing not to be asked whether they want to share each and every time for a set period of time (a sort of opt-out, opt-out option)?

Functionally, both methods impose restrictions on a consumer's ability to elect to share. There may be a multitude of ways to implement sharing functionality. In the end, the appropriate public policy should be aimed at empowering consumers to choose, through an opt-in process, how to share information. The marketplace will experiment with a host of controls and options in an effort to find what consumers want and value.

b. If Congress decided to amend the VPPA to permit customers to opt-in on a continuous basis for a set period of time, what period of time would be reasonable in your mind - three months, six months, a year or some other period of time?

In general, consumer expectations are that once a person has affirmatively made a decision, that decision will not be overridden—by law or any other force—unless and until the consumer affirmatively makes a change.

4. **In your testimony, you stated that as a consumer-driven company, Netflix would always provide consumers with an easy method for withdrawing their consent because that is what consumers want. H.R. 2471 requires opt-in consent to be "informed, written consent ... in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer..." However, this legislation does not specify if a company must provide a clear opt-out option. If Congress were to amend the House legislation, would you support language that would ensure bad actors are not able to make withdrawal of consent difficult for consumers?**

Netflix strongly believes in empowering consumers to act as they wish. Not only does that mean allowing consumers to consent to ongoing sharing if they so choose, but also making it easy for them to change their minds. If a consumer wishes to withdraw his consent to sharing of his movie and TV titles, then Netflix would not think to stand in the way. Nonetheless, we understand that there could be a bad actor in the market that fears it cannot succeed unless its audience is tricked or trapped into using its service. To preempt such a phenomenon, Netflix would support an amendment to H.R. 2471 to include a provision stating that the means for a consumer to withdraw consent must be clear and conspicuous.

5. **In the countries where Netflix already offers their sharing service, can consumers use Netflix's other services without using the application that shares their viewing histories on Facebook or another social network?**

Yes. Netflix subscribers can use our service to discover content and enjoy watching that content on the device of their choosing without any social component. Even if a consumer chooses to use Netflix in a socially integrated manner, that functionality does not require that the movie titles a consumer has watched be published to her Facebook page. By using Facebook's privacy controls, a consumer can prevent movie titles from being published to her wall, or remove them after the fact, while still taking advantage of the benefits of social integration on the Netflix user interface.

6. Should Congress extend the VPPA to cover other "streaming" services or types of media? Why or why not?

The VPPA should not be extended to streaming. Using the VPPA to address broader Internet-focused policies is unwise. It would be far better to begin consideration of broader privacy regulation on a clean slate – that is, do not try to fit the square peg of the VPPA into the round hole of Internet streaming.

Underlying our opinion is what we perceive as a fundamental inability to define streaming in a meaningful and effective way. The concept of "streaming" services is amorphous and dynamic. The lines between different kinds of media have already begun to blur. Take the example of the book, Rawhide Down: The Near Assassination of Ronald Reagan ("Rawhide Down") a detailed documentary of the attempted assassination of President Reagan. Rawhide Down can be read in a bound, paper format purchased from any number of brick and mortar or Internet retailers, all of which may also sell goods in other media formats. Crucially, Rawhide Down is also available as an e-book that has imbedded in its chapters video and audio recordings taken of the attempt itself as well as of interviews of people present that day, and so on. At what point does Rawhide Down become a documentary movie with embedded text versus a book with embedded movies? What if instead of President Reagan's near assassination, the subject of the e-book was the history of the Rolling Stones as recounted primarily through the band's music with some explanatory text – is that a song and album liner sold in an innovative format or is it a book? And what if that e-book had a video of one of the Rolling Stones' concerts – is it then a music video or a movie? In an age of media convergence, attempting to impose the last Millennium's analog definitions on today's reality contorts those definitions.

Even if streaming video could be meaningfully differentiated and defined in the digital dimension, bringing other types of media—such as songs, books, or news articles—under the strictures of the VPPA would fly in the face of clearly demonstrated consumer demand. Media, no matter the format, are vehicles for ideas and expression. People wish to communicate by sharing with others the media they consume. Preventing consumers from engaging in the kind of frictionless social interaction they enjoy and have come to expect would be perceived by those consumers as a constraint on their free expression.

Finally, efforts made by some, including Mr. Rotenberg of EPIC, proposing language that would capture or define "streaming" for the purposes of the VPPA is unavoidably overly broad. EPIC's proposed language would bring within the definition of a "video tape service provider" anyone who disseminates: user generated content, events such as video chat or conferencing, video games, cable or television network content offerings, online education tools and services (which could include educational institutions themselves as the "providers"), and many more. It cannot be the intent of the VPPA to cover an elementary school teacher as a

video tape service provider. Congress should we wary of adopting EPIC's definition into the VPPA because of unintended consequences such as these.

7. **Concerns have been raised that passing H.R. 2471 would allow video tape service providers to disclose the movie and TV titles a video renter has watched to any third party of the video tape service provider's choosing. What, if anything, would prevent video tape service providers from doing this?**

H.R. 2471 does not allow a video tape service provider to disclose video rental history in any manner not already permitted under the VPPA. H.R. 2471 merely enables a consumer to give permission to share what was otherwise permitted on an ongoing basis. The existing protections under the VPPA as to whom disclosure can be made are still applicable.

   a. **If the VPPA is amended in a manner consistent with H.R. 2471, could a consumer unknowingly or inadvertently consent to allowing a video tape service provider to sell information about the movie and TV titles that consumer has watched? Why or why not?**

Again, H.R. 2471 does not change any substantive protections under the VPPA. All it does is provide for a consumer to give ongoing consent and that such consent may be given over the Internet. In fact, H.R. 2471 goes beyond the requirements of the VPPA in its current form, which requires "informed written consent" and adds that the informed written consent must be "in a form distinct and separate from any form setting forth other legal or financial obligations." In this way, H.R. 2471 actually enhances the protections provided by the VPPA by ensuring that consent cannot be buried in some other terms of agreement.

   b. **Does current law prevent this?**

No. Under current law, consumers can consent to such disclosure. As mentioned above, H.R. 2471 actually enhances protection by ensuring that the form of consent be "distinct and separate" from any form setting forth other legal or financial obligations.

Imagine that a consumer goes to a brick and mortar video tape service provider to rent a movie and pays for that rental with a credit card. Current law might not prohibit the store from including language on its credit card receipts—which require signatures—that states by signing the receipt, the video renter consents to the disclosure, of the title for which she has just paid a rental fee, to a third party of the video tape service provider's choosing. By contrast, H.R. 2471 empowers that consumer to be in control of her decision by ensuring that any consent she provides has been presented to her apart from any other legal or financial obligations, thereby eliminating the possibility of unknowing or inadvertent disclosure.

8. Concerns have been raised that allowing on-going consent could result in consumers accidentally disclosing movie or TV titles to friends or family that a consumer might not actually wish to disclose. Does the Netflix app have any safeguards in place to prevent this?

Yes, the Netflix-Facebook integration currently contains a number of features that serve to limit possible accidental disclosure. First, Netflix provides a "Don't Share This" button that can be used on PCs and many other devices. The button appears on the screen when a user launches a movie or TV show and then after some amount of playtime, fades away. Secondly, a movie or TV title will not be shared until a viewer has watched more than 50 percent of the title in question. That gives the viewer time to decide whether she does indeed want to share the title that she is watching. Finally, as discussed above, a consumer will always be able to control what she is sharing on her social network through the privacy controls on that network, including not sharing information to her wall at all, while still enjoying the benefits of social integration from the Netflix side of the experience. Netflix is interested in providing a feature that our consumers use and enjoy. As such, we want to provide appropriate controls to protect consumers' privacy, while also allowing consumers to engage in frictionless sharing, should they elect to so share their video viewing.

RESPONSES OF CHRISTOPHER WOLF TO QUESTIONS SUBMITTED BY SENATOR TOM COBURN

Response of Christopher Wolf
Director, Privacy and Information Management Group, Hogan Lovells LLP
to Written Questions of Senator Tom Coburn, M.D., U.S. Senate Committee on the Judiciary
Submitted February 22, 2012

---

1. **In your testimony, you asserted it would be good policy for Congress to amend the Video Privacy Protection Act (VPPA) to permit consumers to provide on-going consent to share their viewing histories. Why do you believe this is good policy?**

Technology has advanced rapidly to permit individuals to communicate in ways previously unimagined – for example, through social media – and to share information about themselves and their interests. There are people who want automatically and on an ongoing basis to share with their friends through social media what streaming movies they are watching online. The current structure of the VPPA effectively prevents individuals from making an on-going sharing choice that would allow them to share automatically information about the online streaming videos they watch. This is because the major online streaming video providers do not provide that on-going sharing choice for fear of being found in violation of the VPPA. (As discussed at the hearing, there are language ambiguities in the statute that arguably prohibit an online streaming video provider from implementing a consumer's choice to share information about videos watched on an on-going basis.)

The law should be changed to allow consumers to make a choice to share streaming video-watching information on an ongoing basis. Thus, it should be made clear that online streaming video providers will not face legal penalties for providing consumers with that choice.

I am not aware of any other privacy law that restricts what information individuals can choose to share and restricts how, technologically, choices can be made by people to share information. That is the effect of the VPPA today because of its ambiguities and why an amendment clarifying the situation and empowering consumers to make choices they may want to make is called for. Such an amendment removing the potential legal liability for online video services offering consumers an ongoing sharing option would align the VPPA with the preferred technology-neutral and consumer-empowering approach to privacy laws today.

   a. **Why do you believe allowing consumers to give on-going consent is preferable to giving consent each and every time?**

I do not believe that allowing consumers to give on-going consent is preferable to giving consent each and every time. This should not be an either/or situation, in my view. Some people may want to share on an on-going basis information about the online videos they watch, and some people may want to make the decision to share on a per video basis. Both choices should be available to consumers. Again, the key to privacy is control and choice, and so long as consumers have the options available to them, they will have control and the ability to choose.

b. Do companies providing other types of media such as music or books permit a one-time opt-in for customers?

Yes. Two recent, prominent examples that have been integrated into social media include the streaming music service Spotify, which permits users to share the music they listen to via the service, and the Washington Post Social Reader, which permits users to share the articles they read. Both of these web applications permit users to provide a one-time opt-in to share their media-consumption preferences through the service.

c. What would be the difference, if any, between allowing consumers to opt-in to sharing everything for a set period of time as opposed to choosing not to be asked whether they want to share each and every time for a set period of time (a sort of opt-out, opt-out option)?

As I understand it, this question asks about an opt-in for on-going sharing that expires and needs to be renewed, and a default of a per-video sharing choice with an option to make an ongoing sharing choice (rather than a per-video sharing choice) for a set period of time. The preconception here is that consumers need to be reminded they are sharing, because sharing is potentially embarrassing or revealing. As I mentioned at the hearing, if Congress gets into the business of enacting laws to remind consumers when sharing might be embarrassing and revealing, the potential scope is very broad, from web cams to cell phones and beyond.

For a consumer that wants to make a persistent, on-going sharing choice, there is no difference between the mechanisms referenced in the question as each interferes with the consumer's desired outcome and choice. If the suggestion is that the law should require these mechanisms, then I think that is a bad idea, for the reasons previously stated about interfering with the ability of individuals to make choices they want to make, and because of the slippery slope of lawmaking to prevent people from making choices about sharing that could embarrass them or reveal more information about themselves than they may have contemplated. In addition, technologies change, and along with them, choice mechanisms change. A law prescribing choice mechanisms based on today's technology could become outmoded and archaic very quickly. It also could inhibit the development of privacy-enhancing choice mechanisms by imposing strictures.

2. Would every Netflix customer have to use an application that shares their viewing histories on Facebook or another social network if Netflix was able to offer this service in the U.S.?

No. The ability of Netflix or other online video providers to *offer* an on-going sharing choice does not mean that a customer has to use the application to share. There are many people who do not want to share information about the videos they watch online, and merely because an application is available, does not mean those people have to use it. They have a choice *not* to share, just as people who want to share have a choice, and should not be limited in that choice.

3. Should Congress extend the VPPA to cover other "streaming" services or types of media? Why or why not?

The VPPA today is plagued by ambiguity precisely because it attempted to anticipate technological developments but failed to do so effectively. An amendment to cover "streaming" services could result in restrictions on people sharing information about books, magazines or newspapers they have read (or other media not yet in existence) because of the availability of streaming video contained in those media. As Congress considers whether to legislate in the area of privacy, a focus on specific technologies as opposed to broad principles seems ill-advised and inconsistent with global trends.

4. Concerns have been raised that passing H.R. 2471 would allow video tape service providers to disclose the movie and TV titles a video renter has watched to any third party of the video tape service provider's choosing. What, if anything, would prevent video tape service providers from doing this?

This is not the case. H.R. 2471 retains the requirement that video tape service providers obtain the opt-in consent of their customers prior to sharing video-watching information. If the video tape service provider wishes to share video-watching information of a customer with a third party, it must first seek out and obtain the consent of the customer, who is not required to provide such consent. The opt-in consent must be "informed consent," that is, it must be based on a clear, specific disclosure of the scope of the consent. Any provider that fails to provide such a disclosure would not be complying with the law, in my view.

a. If the VPPA is amended in a manner consistent with H.R. 2471, could a consumer unknowingly or inadvertently consent to allowing a video tape service provider to sell information about the movie and TV titles that consumer has watched? Why or why not?

Under H.R. 2471, consent to share video-watching information must be informed and consumers must provide an affirmative manifestation of that consent. By virtue of these requirements, consumers cannot "unknowingly or inadvertently" consent; if a consumer gives informed consent, she is not unknowing. Again, misleading a consumer would be a violation of the law.

H.R. 2471 also requires consumers to provide consent in a form separate from other notices setting forth other legal or financial obligations. This bolsters consumer understanding by ensuring that, consistent with privacy best practices, consumers are not "unknowingly" providing consent to the disclosure of their sensitive information by blindly agreeing to a lengthy legal disclosure that happens to contain a provision authorizing the sharing of their information. The notice of sharing under H.R. 2471 must be separate and distinct.

b. Does current law prevent this?

Currently, the VPPA permits video tape service providers to disclose video-viewing information "to any person with the informed, written consent of the consumer given at the time the disclosure is sought." Again, "informed, written consent" should guard against unknowing or inadvertent consent because it must be informed. H.R. 2471, however, provides an extra protection: the consent must be separate and distinct from other legal notices. In that regard,

H.R. 2471 provides an additional safeguard for consumers by ensuring that their "consent" is not buried in a longer disclosure that they might overlook.

c. Does anything prevent the same concern being raised with other sharing apps such as for book[s] or [music]?

Currently, there is no privacy law expressly preventing businesses from disclosing a consumer's book-reading or music-listening habits to third parties, although reputable businesses routinely disclose these information-sharing practices in privacy policies that consumers can review prior to engaging with those businesses.

5. Is it easy for customers to discontinue using other sharing apps such as Spotify and Washington Post Social Reader?

Reputable social networking platforms provide simple mechanisms to enable consumers to discontinue the use of social sharing apps such as Spotify and Washington Post Social Reader (as they would be able to delete any other app). For example, Facebook users can delete an app by clicking on the "Account Settings" link from any Facebook page, clicking on the "Apps" link, and then selecting apps to delete. For standalone applications not integrated into a social networking platform, the Federal Trade Commission has required such applications to provide a straightforward mechanism enabling consumers to uninstall the application, such as through the operating system's standard "Add or Remove Programs" feature.

a. To your knowledge, have there been any customer complaints regarding the difficulty of opting out or terminating service with any of these sharing apps?

I am not aware of any customer complaints regarding the difficulty of opting out or terminating service with Spotify or Washington Post Social Reader.

WASHINGTON
LEGISLATIVE OFFICE

January 31, 2012

Chairman Al Franken
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
224 Dirksen Senate Office Building
Washington, DC 20510

Ranking Member Tom Coburn
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
224 Dirksen Senate Office Building
Washington, DC 20510

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

RE: ACLU opposes expanded unwarranted law enforcement access to private rental records and broader privacy implications in H.R. 2471

Dear Chairman Franken and Ranking Member Coburn:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to the principles of individual liberty and justice embodied in the U.S. Constitution, we are writing today to express serious concerns regarding H.R. 2471, which curtails the privacy protections of the Video Privacy Protection Act (VPPA). If these concerns are not addressed, we will oppose the bill. The VPPA represents a model of good consumer privacy law and should be mirrored in other statutes rather than undermined. In addition, H.R. 2471 exposes sensitive personal information to greater law enforcement scrutiny. The committee should not consider such targeted special interest legislation when it is actively debating broad new protections for digital privacy, particularly when these changes are unnecessary.

H.R. 2471 amends the VPPA to allow consumers to grant a perpetual consent to the sharing of their video rental records (including movies rented online through companies like Netflix). Currently the VPPA requires consumer's consent each time a company discloses a record. The practical effect of H.R. 2471 would be to reduce consumer control over a sensitive category of personal information, namely video and movie rentals and sales.

The VPPA was enacted in response to the Supreme Court confirmation hearings of Judge Robert Bork. During the course of the confirmation process, a reporter from the *City Paper* gained unauthorized access to Judge Bork's video rental records and attempted to use his personal viewing habits to shape judgments about his character. While the incident involving Judge Bork's records was the most high profile example, testimony from the time demonstrated that video rental records were also

wrongly used for other purposes, including as part of divorce proceedings.[1] At that time, many senators expressed outrage over this practice.[2] Senator Leahy characterized the disclosure of the tapes as "an issue that goes to the deepest yearning of all Americans that we are here and we cherish our freedom and we want our freedom. We want to be left alone."[3]

These incidents proved to be only a precursor to the massive information use and misuse that would follow over the next two decades. We now live in a world of records. Every communication online, every credit card transaction, every borrowed library book creates a record. Our travels are frequently recorded; from EZ Pass to subway fare to cell phone tracking, we leave a trail, frequently an unwilling trail. All of this information can be used in ways we did not intend.

H.R. 2471 exacerbates this problem by reducing consumer control over another category of sensitive, personal information and creates four specific problems.

It will reduce the efficacy of the VPPA. As it is currently drafted, the VPPA is in many ways a model statute. While it only covers a narrow class of records, it does so in an exemplary fashion. In addition to the protections against inappropriate law enforcement access discussed below, the statute carefully governs how video records may be released in a variety of situations. Tricky issues are carefully delineated including sharing information during the ordinary course of business (a defined term under the statute), addressing record requests from civil proceedings, and creating marketing lists.

Violations of the act can be enforced through a civil action, one that includes liquidated damages, punitive damages and reasonable attorneys' fees. Unlawfully obtained information may not be introduced into any court proceeding. Finally, old records must be destroyed within one year after they are no longer necessary for the purpose for which they were collected.

More privacy statutes, especially those governing records, should mirror the VPPA. Undermining it sends the wrong message about privacy protections for transactional records.

It will bypass key protections against law enforcement access. The VPPA contains strong protections against unregulated access to video rental records by law enforcement. Under 18 U.S.C. 2710 (b)(2)(C):

> "A video tape service provider may disclose personally identifiable information concerning any consumer-- ... to a law enforcement agency pursuant to a warrant issued under the Federal Rules of

---

[1] *Video and Library Privacy Protection Act of 1988: Hearing before the Senate Committee on Judiciary*, 100th Cong. 65 (1988) (testimony of Janlori Goldman).
[2] *Id.*
[3] *Id.*

> Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order…"

And then under 18 U.S.C. 2710 (b)(3):

> "Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry."

Even with the passage of H.R. 2471, these protections would continue to apply to video providers (including those renting movies online). However, it is unlikely that a court would require a third party (such as Facebook) to abide by these rules.

Given this fact, and given that sites like Facebook are routinely monitored by law enforcement, the unintended consequence of this legislation will be to give much greater access to this class of records than was intended by Congress when the statute was drafted.[4]

Electronic privacy law is currently in flux. A broad coalition of businesses, consumer and civil liberties groups from across the political spectrum, academics, and others have called for reforms to the Electronic Communication Privacy Act. These groups, known collectively as the Digital Due Process (DDP) coalition, recognize that our electronic privacy laws are badly out of date.[5] Such obsolescence harms civil liberties, prevents businesses from fully exploiting new technologies, and creates confusing and antiquated rules for law enforcement. Current legislation before the committee, including S. 1011, the "Electronic Communications Privacy Act Amendments Act", is aimed at remedying some of these problems. Because H.R. 2471 implicates both business practices and core privacy issues, it is squarely part of that larger debate.

As we described recently to the full committee in a statement regarding S. 1011, transactional records of the type covered by the VPPA must be part of the discussion. Records of where consumers go online, what they read and purchase, and with whom they communicate are often more sensitive than the actual contents of their communications.[6] Microsoft similarly argued that it has a vital interest in another technology, cloud computing. According to Mike Hintz, Associate General Counsel at

---

[4] Morran, Chis. ""NYPD Forms New Unite to Monitor Facebook and Twitter for Signs of Criminal Activity." *The Consumerist*, 10 Aug. 2011. http://consumerist.com/2011/08/nypd-forms-new-unit-to-monitor-facebook-and-twitter-for-signs-of-criminal-activity.html

[5] A complete list of DDP members can be found here: http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163

[6] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing before the Senate Committee on Judiciary*, 111th Cong. 47-56 (2010) (written statement of the American Civil Liberties Union).

Microsoft, "Users of cloud services must have confidence that their data will have privacy protections from government and from providers," and his company "regularly hears from enterprises that moving data to the cloud affects privacy."[7]

Committee Chairman Patrick Leahy eloquently stated in recent comments, "I introduced legislation to update the Electronic Communications Privacy Act, so that this law remains viable in the digital age. Congress must now do its part to enact this legislation, so that our federal privacy laws keep pace with technology and protect the interests of our nation's citizens, law enforcement community, and thriving technology sector."[8] Passing piecemeal legislation runs completely counter to that objective and will likely result in the perpetuation of an uneven playing field both for privacy and new technologies.

It is unnecessary. Sharing of personal information, like video rental records or other transactions, is currently extremely easy. For example, after consumers complete a transaction on the web retailer Amazon.com, they are presented with a screen which confirms the sale and allows them to share the fact of their purchase through Facebook, Twitter or other social media. In fact, the post is already prepared and "I just purchased [item]" appears in the body of the message or tweet. The consumer simply has to click a button and the message is sent.

It is difficult to imagine how this could be any easier for consumers. They are completely empowered to share their purchases whenever they want. Most importantly, they control whether they share a particular purchase or rental. The process a consumer would have to undertake if H.R. 2471 becomes law presents a sharp contrast. Once consumers agree to share information, they would have to decide each time whether they want to keep information private and hunt down the method for disabling sharing.

As currently drafted H.R. 2471 raises serious concerns regarding consumer control and law enforcement access to video records and has a detrimental impact on other important policy decisions currently pending before the committee. If the committee does not address these concerns before taking any action on H.R. 2471, we will oppose the legislation.

Sincerely,

Laura W. Murphy

---

[7] Howard, Alex. "ECPA reform: Why digital due process matters." *O'Reilly Radar*, 23 Sept. 2010. http://radar.oreilly.com/2010/09/ecpa-reform-why-digital-due-pr.html

[8] Press Release, Office of Senator Patrick Leahy, Comment Of Senator Patrick Leahy (D-Vt.) Chairman, Senate Judiciary Committee, On Supreme Court Decision In *United States v. Jones* (Jan. 3, 2012).

Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

16530 Ventura Boulevard
Suite 400
Encino, California 91436-4551
Voice 818.385.1500
Fax 818.385.0567
www.entmerch.org

December 13, 2011

The Honorable Lamar Smith
Chairman, Committee on the Judiciary
2138 Rayburn House Office Bldg
U.S. House of Representatives
Washington, DC 20515

RE: Video Stores Are Not "Obsolete" (H.R. 2471, H. Rpt. 112-312)

Dear Mr. Chairman,

I am writing as the President and CEO of the Entertainment Merchants Association, the national trade association for the retailers and distributors of DVDs, Blu-Ray Discs, and video games to correct two misstatements in House Report 112-312, which accompanied H.R. 2471, the Video Privacy Protection Act amendment.

H. Rpt. 112-312 (page 2) states:

> Today, not only are VHS tapes obsolete, so too are traditional video rental stores. The Internet has revolutionized how consumers rent and watch movies and television programs. Video stores have been replaced with ''on-demand'' cable services or Internet streaming services....

Notably, the statements that video stores are obsolete and that they have been replaced by cable and internet video-on-demand were published in the Report without attribution. Nor can there be any citations, as the statements have no basis in fact. The truth is that, at the end of 2010, there were approximately 11,000 video rental stores around the nation providing affordable, quality entertainment on DVD and Blu-Ray Discs to millions of Americans.

Enclosed please find EMA's latest *D2: Discs & Digital – The Business of Home Entertainment Retailing* report. As noted in the report (page 17), although online video subscription services such as Netflix and rental kiosks such as Redbox captured 42% and 22% of the rental market in 2010, respectively, traditional video rental stores still accounted for 36% of the market. While innovative channels for delivering rental video have been enthusiastically embraced by consumers and are expected to continue to gain market share, it is simply not accurate to declare traditional rental stores "obsolete." We anticipate that a significant segment of consumers will remain loyal to the convenience, selection, and value of traditional video rental stores for the foreseeable future.

With respect to the inaccurate statement that "[v]ideo stores have been replaced" by digital distribution channels, the *D2: Discs & Digital* report also makes clear that packaged media, such

as DVDs and Blu-Ray Discs, continues to dominate the video market. As the pie chart on page 14 demonstrates, packaged home video accounted for 42% of the consumer motion picture and video spending in 2010, while cable and internet video-on-demand and other forms of digitally delivered home video represented only 5% of consumer video spending. In 2010, spending on packaged video entertainment (sales and rentals) totaled $16.2 billion.

While the DVD market has declined since the halcyon days after its arrival in the market, Blu-Ray Disc sales increased 53% last year and Blu-Ray rentals were up 34% in brick and mortar rental stores. EMA agrees that the Internet is revolutionizing the home entertainment market, and our members embrace digital distribution and realize it will be a significant component of our industry in the coming years. At this point, however, it is wholly inaccurate to state that cable and Internet video-on-demand have "replaced" packaged home video.

While we realize that H.R. 2471 has already passed the House of Representatives, we did not want these statements to go by uncorrected. We hope that these statements will not be repeated and that there will be an opportunity at some point in the future to correct the record.

Entertainment Merchants Association

The Entertainment Merchants Association (EMA) is the not-for-profit international trade association dedicated to advancing the interests of the $35 billion home entertainment industry. EMA-member companies operate approximately 35,000 retail outlets in the U.S. and 45,000 around the world that sell and/or rent DVDs, computer and console video games, and digitally distributed versions of these products. Membership comprises the full spectrum of retailers (from single-store specialists to multi-line mass merchants, and both brick and mortar and online stores), distributors, the home video divisions of major and independent motion picture studios, video game publishers, and other related businesses that constitute and support the home entertainment industry. EMA was established in April 2006 through the merger of the Video Software Dealers Association (VSDA) and the Interactive Entertainment Merchants Association (IEMA).

Thank you for the opportunity to provide this information.

Sincerely,

Crossan R. Andersen
President & CEO

Enc.