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 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 ("FTC")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 customers' video viewing histories 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 General Services Administration, 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 safeguards 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 the 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 to Data and Logic 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