KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

March 15, 2011

Committee on Judiciary I – Civil Law
Stratton Building
Springfield, Illinois 62701

Re: House Bill 3280: Internet Service Provider Anti-Child Pornography Law

Dear Chairperson Nekritz, Representative Kay, Representative Bellock, and Members of the Committee:

The Center for Democracy & Technology (CDT)[1] appreciates the opportunity to present to the Committee on Judiciary our concerns about House Bill 3280, the Internet Service Provider Anti-Child Pornography Law ("the Act"). We share the legislature's concern about the sexual exploitation of minors. This bill, however, raises serious constitutional concerns and a range of extremely burdensome technical problems. If passed, it would be vulnerable to court challenge.

HB 3280 would require an Internet Service Provider (ISP) that has any customers in Illinois to create and implement software to intercept any browsing activity on the World Wide Web,[2] any file attached to an email, or any request to examine a file menu using file-sharing software. The software would then compare the information accessed or requested against a registry of "hash values" of images that are "known to contain child pornography." If the file or request for a file matches a hash value in the registry, access to the file must be blocked and a replacement file delivered, warning the customer that the blocked file is illegal.

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. CDT is one of the leading civil liberties organizations in the United States focused on the application of the U.S. Constitution's First Amendment to speech on the Internet. CDT has offices in Washington, D.C., and San Francisco.

[2] We interpret the language of Section 23-110(c)(1), "[w]henever a customer searches the Internet through the World Wide Web," to cover any web browsing that a user does. If this language in fact only applies to the results of queries entered by a user into search engines, the technical and speech burdens discussed below would still apply, and the bill would also fail to capture files on websites that users access directly by entering a URL.

I. Legal Issues

HB 3280 raises very serious constitutional and legal issues. The Act directs ISPs to filter user content based on a global file registry that does not currently exist. Creating such a registry would raise serious First Amendment concerns over government blacklists and prior restraints on speech. If the state intends to use a list created by an organization such as the National Center for Missing and Exploited Children (NCMEC), it will raise significant Due Process Clause problems, as the lists maintained by such organizations include "apparent" (not "adjudicated") child pornography, are not created via a transparent or reviewable process, and are, in any event, ostensibly *privately* developed assessments of the legality of content that cannot form the basis of state action. Further, the technical implications of process described in the Act would significantly burden Illinois residents' speech, slowing the speed of Internet communications to a crawl, and prohibiting certain types of communication altogether. The process described would also likely violate the Fourth Amendment prohibition on unjust searches and would run afoul of the Electronic Communications Privacy Act.

First Amendment

While sexually explicit images of minors do not receive First Amendment protection, the filtering process mandated in HB 3280 nevertheless raises significant problems under the First Amendment of the Constitution. Section 23-110(b) of the Act instructs the Commission to select a nationwide law enforcement agency to provide a list of hash values of files "known to be child pornography." It further instructs that "[t]he selected law enforcement agency shall inspect the files and makes [sic] a judgment that the files are illegal in their jurisdiction." But the First Amendment does not permit law enforcement, acting alone, without benefit of a judge and jury, to designate particular content as illegal and require or encourage ISPs to block it. Material must be adjudicated to be child pornography following a court proceeding with full due process protections; absent these protections, such a list is the equivalent of a government blacklist of content that cannot survive constitutional scrutiny.[3]

It is not clear which "nationwide law enforcement agency" Illinois might select to serve as a clearinghouse for the list of illegal images. The National Center for Missing and Exploited Children (NCMEC) is an organization that collects reports of apparent child pornography and forwards those reports to federal and state law enforcement agencies. But NCMEC's list may not be used to implement HB 3280, for several reasons. First and foremost, NCMEC does not, and is not in any position to, make any "judgment" of illegality (as HB 3280 envisions). All NCMEC does is refer images that are suspected of being illegal images of minors to law enforcement agencies for review.

[3] Bantam Books v. Sullivan, 372 U.S. 58 (1962). See also Ctr. For Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (striking down blacklists of websites).

Moreover, there would be very serious constitutional concerns if Illinois did decide to rely on any list or database prepared by NCMEC. If NCMEC is viewed as a "nationwide law enforcement agency," and therefore an arm of the government, the same government-blacklist concerns apply to NCMEC's list of apparent child pornography. Treating NCMEC as a non-governmental organization, however, does not alleviate the constitutional concerns: NCMEC's list is created and maintained in a purposely non-transparent manner – the public cannot view the list of images, and no judicial or other review or appeal process tests NCMEC's determinations. When the output of NCMEC functions merely as a tool for law enforcement to conduct further investigations, these limitations on access to NCMEC's list may be appropriate. But the State of Illinois cannot order ISPs to block content based on an unreviewable list maintained by a private entity that offers no opportunity for a full adjudication with constitutionally guaranteed due process rights. Furthermore, the government cannot in any event "outsource" to a private entity the determination of what content might be illegal.[4]

Even if a global file registry only includes images that have been adjudicated to be child pornography (although no such registry exists), the Act would place an egregious burden on constitutionally protected speech. As we discuss in more detail in Section II, the technical process envisioned by this bill would prohibit certain types of legal, constitutionally protected speech (such as encrypted communications), would introduce significant privacy and cybersecurity concerns that would chill users' speech, and would dramatically slow the speed of Internet-based communications for all Illinois residents. Thus, the fact that HB 3280 addresses illegal material does not save it from First Amendment scrutiny.

Commerce Clause

The Act would also run afoul of the Commerce Clause of the Constitution, as it places an excessive burden on interstate commerce.[5] While combating child pornography is a compelling state interest, federal courts routinely conclude that state laws that directly regulate the Internet place excessive burdens on

---

[4] *See, e.g.*, Entertainment Software Ass'n v. Hatch, 443 F. Supp. 2d 1065, 1071 (D. Minn. 2006) (finding state's use of private Entertainment Software Ratings Board's ratings system as basis for determining whether to assess a fine was violation of Fourteenth Amendment's Due Process Clause); Eastern Federal Corporation v. Wasson, 316 S.E. 2d 373 (S.C. 1984), (holding that tax of 20 percent on all admissions to view movies rated either "X" or unrated was an unconstitutional delegation of legislative power to a private trade association); Swope v. Lubbers, 560 F. Supp. 1328 (W.D. Mich. 1983) (finding use of motion picture rating system was improper as basis for determination of constitutional protection); Drive-In Theater v. Huskey, 435 F.2d 228 (4th Cir. 1970) (enjoining sheriff from prosecuting exhibitors for obscenity based on "R" or "X" rating).

[5] Pike v. Bruce Church, Inc. 397 U.S. 137, 142 (1970) (holding that a state statute that does not explicitly discriminate against interstate commerce can nonetheless be found to violate the Commerce Clause if it imposes a burden on interstate commerce that "is clearly excessive in relation to the putative local benefits" achieved by the statute).

interstate commerce.[6] Due to the extensive technical issues with the bill outlined below, HB 3280 would significantly limit, and in some cases completely prohibit, Illinois (and in some cases out-of-state) residents from using the Internet to communicate and engage in commercial transactions.

Further, it is not clear that the Act would achieve the state's interest in reducing access to child pornography within the state. The Act directs ISPs to block images based on the hash value of a file listed in the global file registry. A hash value is computed based on the specific characteristics of a given file and is unique to that file; if even a single pixel of an image is altered, that file will generate a different hash value. This makes hash value-based filtering of child pornography easy to circumvent and renders HB 3280 ineffective at achieving the state's interest.

Finally, the Act is likely to be deemed per se invalid under the Commerce Clause for its extraterritorial effects. Because ISPs' networks typically cross state boundaries, an ISP with servers in Illinois could be required to apply Illinois state law to communications occurring wholly outside the state's boundaries.

Other Legal Issues

Beyond the constitutional concerns under the First Amendment and the Commerce Clause, HB 3280 would also raise serious Fourth Amendment concerns, in that the state would require searches of almost all online communications of all Illinois residents, based on no level of suspicion whatsoever, with no legitimate claim of probable cause.

Further, ISPs complying with the Act would likely be in violation of the federal Electronic Communications Privacy Act (ECPA). ISPs would need to reassemble every communication – email, request for a web page, instant message communication, file download – sent by Illinois residents in order to determine which communications were of the types that must be examined under the Act. ECPA prohibits ISPs from intercepting and examining the contents of users' communications in this way.[7] While the Act attempts to make a distinction between the ISP computing a hash value for a file and "examin[ing] the content of the file", ECPA does not recognize any such distinction between a human physically examining a particular file and an ISP reassembling packets and analyzing their contents.[8]

---

[6] PSInet v Chapman, 362 F.3d 227, 240 (4th Cir. 2004); ACLU v. Johnson, 194 F.3d 1149, 1160-61 (10th Cir. 1999); ALA v.Pataki, 969 F. Supp. 160, 177-81 (S.D. N.Y. 1997).
[7] 18 U.S.C. 2511(3).
[8] 18 U.S.C. 2510(8) ("'contents' . . . includes any information concerning the substance, purport, or meaning of that communication").

II. Technical Issues

While some of the technical issues the Act presents could be addressed through revisions to proposed definitions, the basic process the bill envisions – requiring ISPs to analyze users' traffic as it passes over the ISP's network – is inherently problematic. As a starting point, ISPs' networks do not currently transmit information in a way that makes this kind of monitoring and analyzing of user traffic possible. To transmit information via the Internet, individual files are broken down into small elements called "packets" that are sent individually by the user's personal computer through the network and then reassembled at the destination computer or server. Different packets take different routes to the destination, passing through different nodes of the ISP's network. To compute the hash value for a file, an ISP would need to collect every packet that comprised the file at a single point within the network. This shift – away from a distributed communications network toward a network with a single point of control – would represent a major change in how ISPs transmit information over their networks and would introduce significant inefficiencies to Internet communications.

Essentially, this Act would require an entire re-architecting of the Internet, which would create huge disruptions for companies seeking to service Illinois customers, would generate significant costs for those companies and their customers, and would almost certainly reduce the ability of smaller service providers to remain in business (which would, in turn, reduce competition and thereby drive up prices for consumers even further). These disruptions alone would be sufficient foundation for a constitutional Commerce Clause challenge, as discussed above. Illinois simply cannot order a complete redesign of Internet communications.

Moreover, ISP efforts to comply with HB 3280 would lead to significantly slower Internet communications for Illinois residents. Consider a simple visit to a news website: A user's visit to the home page of, for example, cnn.com or foxnews.com involves the download of more than 100 separate "files," each of which would have to be intercepted, reassembled, analyzed, compared to the hash value database, and only then transmitted to the end user. This process, which the ISPs would have to undertake for each and every web page that every single user visited, would have a significant harmful impact on *all* web browsing in Illinois, limiting Illinois' residents' opportunities to speak and to access information.[9]

Along the same lines, Section 23-110(c)(1) orders ISPs to compute hash values for every file listed in a menu on a peer-to-peer network. In order to do this, the ISP would first have to join the peer-to-peer network, possibly paying money to do so, and download every available file to its own servers. This will cause a significant delay in returning the user's request to begin downloading any files. In a world where Google calculates the length of time it takes to return search

[9] This impact alone would almost certainly lead some companies to choose to locate in states that did not require such significant interruption of all Internet access.

results by milliseconds, even brief delays in transmission of data will have a noticeable negative impact on the user's experience. HB 3280 would cause far more significant delays.

In addition, ISPs would be faced with the choice of banning their users from using encrypted communications or risk not complying with the Act. Many important transactions occur through encrypted online communication: Any time a person accesses a website address beginning with "https://", such as when checking a bank account or paying a utility bill, that transaction is encrypted. The purpose of encryption is to prevent any third party, including the ISP that transmits the communication, from being able to examine the data that is transmitted. An Illinois ISP would not be technically capable of assembling a file transmitted over an encrypted connection, and thus would not be able to compute the hash value of that file in order to comply with the Act. ISPs would have to technologically prohibit their customers from sending or receiving encrypted communications. This will make Illinois residents significantly more vulnerable to cybersecurity threats and identity theft. Many popular websites and online services, including Facebook and Gmail, routinely encrypt their users' communications to provide greater security and privacy. Illinois ISPs would have to prohibit their users from using the encrypted versions of these services.

Finally, implementation of the Act would render impractical, or even impossible, a wide range of Internet-based communications that rely on speed, security, and distributed processing to function. Tele-work, which at many companies requires encrypted "virtual private networks" that could not be permitted under HB 3280, would no longer be possible for many workers in Illinois. Web sites that provide streaming video – such as YouTube – would no longer work in Illinois. A broad range of other tools, including communications innovations that have yet to be invented, would pass by the state of Illinois.

* * *

As a final consideration, we note that litigation to defend unconstitutional laws is extremely expensive for a state. Because the Act plainly violates the First Amendment and Commerce Clause of the U.S. Constitution, a legal challenge is sure to follow if HB 3280 is enacted into law, and the costs to the taxpayers of Illinois to defend the law will be high. Over the past 12 years, in 14 constitutional challenges to regulations of the Internet and other new technologies, the average cost to the government (in both fees paid to plaintiffs' attorneys and the cost of defense) has been in the neighborhood of $500,000. We suggest that a far more effective use of those funds would be to appropriate money for Illinois law enforcement, at the state level and in coordination with federal law enforcement agencies, to investigate and prosecute child pornography trafficking and child exploitation crimes. That approach would be more effective, less damaging, and more constitutional than the approach proposed in HB 3280.

We appreciate the opportunity to present our views to the Committee. We would be happy to provide any additional input or briefing that might assist the Committee.

Sincerely,

/s/

John B. Morris, Jr.
General Counsel
Center for Democracy & Technology