See No Evil: The Threat to Individualism and Open Forum

Eric Webb

Kansas State University

Executive Summary

As technology advances, more and more people are using the internet for day to day activities. Along with regulations the service providers enforce, the Federal Government has laws that help protect providers of interactive computer services from being held liable for what a user posts, and how a provider structures their service. Users of a provider's service aren't always law-abiding, which have sparked recent calls to have better surveillance of these public services. The surveillance and further regulation of their services threatens the first and fourth amendment rights of their users, as well as the liability protection of the service providers.

Introduction

At the dawn of the internet, the Communications Decency Act (CDA) was passed by congress in order to protect new business ventures in the digital world. Section 230 of the CDA protected you and your company from any liability for what your customers might do with your service. The government trusted you to moderate your site and stayed out of your way while you jumped feet first into the 21st century. Currently, there are talks from the government to revoke your protection and penalize your company if you don't build it in a way that is easily monitored. What if you, as a business entity, decide that you don't think the government best practices (rules or procedures that are accepted as either "correct" or "most effective") are appropriate for you? Upon failing to meet their requirements, the government will penalize you.

History of Technology and Privacy

The 1928 Supreme Court case Olmstead v. The United States set the initial privacy standard. While Olmstead and his lawyer argued that a wiretap violated his fourth amendment rights, the Supreme Court ruled that there was no physical trespass onto his personal property, and therefore didn't count as a search (Bellia, 2006). The ruling in the Olmstead v. The United States case held for nearly forty years until Katz v. The United States (1967). Katz had been caught gambling by the FBI with the use of hidden microphones in a telephone booth. Katz and his lawyer pleaded that their

privacy had been violated. After much deliberation, the court overturned the ruling of Olmstead v. The United States, deciding that "eavesdropping is subject to Fourth Amendment restrictions and that conversation can be 'seized'" (Katz v. United States, 1967).

Katz v. The United States also gave birth to the "Expectation of Privacy" test. Justice Harlan proposed two questions: Has an individual exhibited an actual (subjective) expectation of privacy? If so, is the expectation is one that society is prepared to recognize as reasonable? If both are true, then the government has violated an individual's fourth amendment rights (Katz v. United States, 1967)).

Due to distracted driving accidents, Martin LaLonde, a Vermont House Representative, proposed a bill in January of 2016 that would allow a police officer to search a person's phone during a traffic stop. The idea was to see if the person had been using their phone while driving and allow police to punish it. Technology developed by companies like Cellebrite would be available to police officers. This technology was used to unlock a terrorist's iphone after an attack and proved to be successful (Schober, 2016). Such power in the hands of an officer violates expectation of privacy and for that reason, the bill was shot down.

The EARN IT Act

"Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020," or "The EARN IT Act," was presented to congress on March

third, 2020. The purpose of The EARN IT Act is "To establish a National Commission on Online Child Sexual Exploitation Prevention, and for other purposes" (EARN IT, 2020). Senator Lindsey Graham [R-SC] is the bill's sponsor, and she hopes the passage of this bill would better enable web service/application surveillance and enable the government to quickly remove any child pornography that could be posted.

Passage of the EARN IT Act would give the government full permission to search and scan through user accounts without a warrant or probable cause (Cope, Mackey & Crocker, 2020). A private profile that's supposed to only be seen by a user's friends and family could be read through by government agencies making sure there is no child pornography. Looking through a private profile violates expectation of privacy, as the user has exhibited an expectation of privacy, and the public would agree that the expectation is justified. Given the violation of expectation of privacy, the bill is a clear violation of the fourth amendment.

Currently, there is already a procedure in place for service providers who learn of a violation of child pornography laws. If a provider learns of child pornography, they're required to file a report to the National Center for Missing and Exploited Children's (NCMEC) CyberTipline. The NCMEC then forwards the information to the proper authorities (Cope et al, 2020). If the EARN IT Act is passed, a committee will be formed to perform the following duties:

(A) preventing, identifying, disrupting, and reporting child sexual exploitation;

(B) coordinating with non-profit organizations and other providers of interactive computer services to preserve, remove from view, and report child sexual exploitation;

(C) retaining child sexual exploitation content and related user identification and location data;

(D) receiving and triaging reports of child sexual exploitation by users of interactive computer services, including self-reporting;

(E) implementing a standard rating and categorization system to identify the type and severity of child sexual abuse material;

(F) training and supporting content moderators who review child sexual exploitation content for the purposes of preventing and disrupting online child sexual exploitation;

(G) preparing and issuing transparency reports, including disclosures in terms of service, relating to identifying, categorizing, and reporting child sexual exploitation and efforts to prevent and disrupt online child sexual exploitation;

> (H) coordinating with voluntary initiatives offered among and to providers of interactive computer services relating to identifying, categorizing, and reporting child sexual exploitation;
>
> (I) employing age rating and age gating systems to reduce child sexual exploitation;
>
> (J) offering parental control products that enable customers to limit the types of websites, social media platforms, and internet content that are accessible to children; and
>
> (K) contractual and operational practices to ensure third parties, contractors, and affiliates comply with the best practices.

Sections A-D are already required by law, as organizations must forward the information to the NCMEC. Section F mentions moderating services and reporting and incidents. As the law already requires that service providers make child pornography reports, they all have some form of moderation, including user report features. Users voluntarily being able to report content fulfills the requirements of section H. Age systems have shown to be very poor controllers, as simply clicking “yes” proves you’re over 18. Most sites have done away with such nonsense, as a driver's license would be the only true way to prove your age, at the cost of the massive privacy risk of having that on file. Due to that fact, section I is pointless. Parental controls are widely available and easy to implement already, with very little research

required to fulfill the requirements of section J. Due to the implications of withholding reports, service providers already do their best to comply with the current regulations, as required by section K. In fact, 18.4 million reports were filed in 2018 alone, more than proving that service providers are already doing their part (NCMEC, 2020).

In section six, subsection a of the EARN IT Act (2020), section 230 of the Communications Decency Act is to be amended to selectively grant a service provider liability immunity only in two circumstances:

> "(i) an officer of the provider has elected to certify to the Attorney General under section 4(d) of the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 that the provider has implemented, and is in compliance with, the child sexual exploitation prevention best practices contained in a law enacted under the expedited procedures under section 4(c) of such Act and such certification was in force at the time of any alleged acts or omissions that are the subject of a claim in a civil action or charge in a State criminal prosecution brought against such provider; or
>
> (ii) the provider has implemented reasonable measures relating to the matters described in section 4(a)(3) of the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, subject to the exceptions authorized under section 4(a)(1)(B)(ii) of that Act, to

> prevent the use of the interactive computer service for the exploitation of minors."

Passage of the EARN IT Act as it is would allow the government to force service providers to comply under the threat of having their legal protection removed. Citing the case "Elrod v Burns," Cope, Mackey, and Crocker argue that "the government may not condition the granting of a governmental privilege on individuals or entities doing things that amount to a violation of their First Amendment rights." Granting immunity to some providers, while revoking it from others would be in violation of the Supreme Court's ruling, and therefore unconstitutional.

Closing Thoughts

No matter where in history you look, whether it be the past or the future, there will always be problems. Problems should always be addressed, but they should be carefully studied before proposing a solution. In the case of service providers and their users, it's critical to remember that their rights need to be maintained above all else. Providing liability protection to service providers protects them from being sued due to one user making another uncomfortable. The service can continue to run and users can continue to debate, protecting their first amendment rights.

As for dealing with problems, there are always ways to fix them. Providing benefits to service providers who actively search for and remove content like child pornography doesn't revoke any rights from a company that can't. Providing benefits to the users who use the service every day and see what thousands of people are posting would be even easier. A popular service provider will never have more employees than users, but their users would be motivated to do their work for them, if the user benefits in some way. The internet is too essential to be liable for everything the users do. With every business using some online service, protecting service providers is the only way to protect the users rights.

References

Bellia, P. L. (2006). The fourth amendment and emerging communications technologies. *IEEE Security & Privacy, vol. 4, no. 3,* 20-28. Doi:10.1109/MSP.2006.80

Cope, S., Mackey, A., Crocker, A., (2020). The EARN IT Act Violates the Constitution. Retrieved from https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution

Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT), S.3398, 116th Cong. (2020) Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

Katz v. United States. (1967). *389 U.S 347,* 347-389. Retrieved from http://cdn.loc.gov/service/ll/usrep/usrep389/usrep389347/usrep389347.pdf

NCMEC Data. (2020). Retrieved from https://www.missingkids.org/ourwork/ncmecdata#bythenumbers

Schober, S. (2016). Technology Versus Privacy Issues Preventing Distracted Driver Accidents [Point of View]. in *Proceedings of the IEEE, vol. 104, no. 5,* 896-898. Doi:10.1109/JPROC.2016.2550138