

---

**University of Louisville**

---

# **Final Report**

Do Convicted Hackers Still Have the Right to Internet Access?

Team Seven

Jackson Dillingham, Matthew Jackson, Hilton Siaffa, Tabor Payne, and Emily Wantland

CIS 481-50

# Table of Contents

|              |  |       |
|--------------|--|-------|
| <b>I.</b>    | Executive Summary  | 3     |
| <b>II.</b>   | Introduction and Ethical Question                              | 3-4   |
| <b>III.</b>  | Background on the Right to the Internet                        | 4     |
| <b>IV.</b>   | Users of the Internet and its Role in our Lives                | 4-6   |
| <b>V.</b>    | Who is Restricted from Using the Internet                      | 6-7   |
| <b>VI.</b>   | Alternative Courses of Action such as Temporary Bans or Trials | 7-9   |
| <b>VII.</b>  | Supreme Court Decision   | 9     |
| <b>VIII.</b> | Teleological Perspective                                       | 10-11 |
| <b>IX.</b>   | Deontological Perspective                                      | 12-13 |
| <b>X.</b>    | Normative Recommendation for the Ethical Dilemma               | 13-14 |
| <b>XI.</b>   | References   | 14-16 |

## **I. Executive Summary**

The internet was first created in the late 1960s and more than half of the world population can access the internet. The United Nation believes that Internet access is a human right and it is something that must be protected. The Internet has evolved tremendously since the sixties and allows us to do a multitude of things including online shopping, staying connected with social media, online education, and enjoying entertainment and media.

Various stakeholders have a lot to lose when it comes to the Internet being restricted. These groups include, but are not limited to, felons, society, the government, international organizations, and the technical community. Each use the Internet to their benefit, it would be detrimental to their operations if this use were restricted.

In today's world, we are dependent of the internet and living without it would pose a multitude of challenges. Some individuals are forced to make that adjustment. Thus, felon's punishments should be based on the severity of the crime. Some alternative solutions include being supervised through monitorization or restricted access. This ensures they are not fully banned from the internet and their quality of life isn't impacted.

This ethical analysis focuses on two contrasting ethical perspectives, teleology and deontology. To perform the analysis, we will look at a Supreme Court decision that has ruled the lawfulness of an internet ban. With a teleological view, we are going to analyze each party that would be affected by the decision and determine whether or not the added benefits are greater than the drawbacks. To analyze from a deontological point of view, we have to look at the rights of people and whether or not they are being violated.

## **II. Introduction and Ethical Question**

The internet plays a role in the greater majority of our everyday lives. People have the right to broadband or the freedom to connect. Internet access must be broadly available, and access cannot be unreasonably denied. That said, those guilty of crimes involving the internet have had this access restricted.

Hackers, like any other convicted criminal, will have served their time and reached the point of rehabilitation. Should they be discriminated against? Who has the power to decide that someone doesn't deserve this access anymore?

### **III. Background on the Right to the Internet**

The Internet is a global system of interconnected computer networks that use the internet protocol suite. This is what enable billions of devices to be connected worldwide. In 2016, the UN declared that "online freedom" is a "human right" and that it must be protected. The right to the internet was created in the form of resolution A/HRC/32/L.20 due to the lack of access and suppressive tactics used by certain governments. Several countries throughout the world rejected this resolution including Russia, China, and South Africa. Even though A/HRC/32/L.20 was passed, it is not enforceable because it is a "soft law" and not a "hard law". A soft law recommends actions for nation-states but lacks any enforcement mechanisms.

Although the right to the internet must be protected, around half of the world's population still doesn't have access to the internet. According to a UN report, Asia and Africa have the lowest rates of access (Sandle). According to a UPI report, of the 7.8 billion people in the world, 4.6 billion, or 58 percent, are using the internet. Europe has the world's highest rate of connectivity, with nearly 80 percent of their population online, while Africa has the lowest percentage, with about 21% of their population having internet access (UPI).

### **IV. Users of the Internet and its Role in our Lives**

The very idea of the Internet is important to many different groups of people around the world. We have established five main stakeholders as users of the internet, people that have committed a crime involving the Internet, the government, society, international organizations, and the technical community (Kurbalija). A stakeholder "is a person who has an interest in or investment in something and who is impacted by and cares about how it turns out" (YourDictionary). These five groups have an impact and a say on how Internet access is utilized in their country.

First, we have the government and society. The government can affect society as much as society can affect the government. Individuals mainly use the Internet to help with their daily needs such as looking up information on a specific topic or to purchase a specific item. In East Asia alone, the number of Internet users was 1 billion people in 2019. The second highest is Southern Asia at nearly 800 million users (Clements).

Over the past 30 years, internet usage has surged all around the world. It has become a necessity in our everyday lives. When the internet was created, it was used for military purposes and then eventually expanded for the purpose of communication among scientists. Presently, communicating online through social media has sparked a new way to use the Internet. According to Statista, in 2019, an estimated 2.95 billion people were using social media worldwide, a number projected to increase to almost 3.43 billion people.

Not only has social media changed the way that we use the Internet, but the Internet has also changed the way students are taught, the way we make new purchases, the way that we entertain ourselves, and the way that we receive a limitless amounts of information. According to Education Beyond Borders, the internet has enhanced the education process in several ways. This include lesson enhancement, communication, and convenience. Lessons are enhanced because teachers can give their students extra resources, study materials, and often education games to play. The Internet allows students and teachers to communicate instantaneously. It also offers convenience in terms of taking classes online. This can be extremely helpful for adults that may have a job during the day and are not able to make it to a campus in order to take classes. Instead, they can complete everything online in the comfort of their own home.

From an e-commerce standpoint, a portion of the money spent on the Internet by society goes back to the government in the form of taxes. E-commerce, at least in the United States, is a large part of the economy. In 2019, there was a total of nearly \$602 billion spent on e-commerce (Davis). According to Statista, an average of about \$135 and \$100 is spent on an order through a desktop and phone,

respectively. Without the Internet, the government would be losing a source of capital and society would lose a method to acquire resources and information.

International organizations can include any group that utilizes the Internet to purchase goods for their themselves and advertise their products or services. The technical community can be defined as those behind the creation of the Internet and its maintenance. Both stakeholders rely on the Internet to profit from their businesses. Without the right to Internet access, international organizations would not have the ability promote their business online. Without the technical community, the Internet would not exist. Lastly there are those that have committed a crime using the Internet. They are on the outskirts, and are forgotten by the rest.

Overall, there is a lot at stake when it comes to Internet access. In today's world, so many people and organizations rely on the Internet to make it through the day or to make their business a success. It is important to note that it can be possible for people to make a transition to a non-Internet type of living. However, we have seen over the years that the Internet is more of a positive for people than a negative and no matter what, the Internet's use will only become more prevalent.

## **V. Who is Restricted from Using the Internet**

Convicted hackers are felons. When caught, they earn specified penalties for breaching criminal law. The Computer Fraud and Abuse Act prohibits an individual from accessing a computer without authorization. However, this bill was enacted in 1986. The world today cannot support such a reaching punishment. Today, humans are dependent on the use of internet and technology. We use computers and phones as forms of entertainment, GPS, for education, to pay bills, making purchases, for socializing, for working, and so much more.

Higinio Ochoa, a member of Anonymous, was arrested and imprisoned for hacking police websites to expose officers engaged in police brutality. As a further punishment, he was ordered to live an internet-free life. Though he may be content now, he has his wife to help him navigate the world (Bertrand). Without someone to act as his physical hands, this simply isn't realistic.

Kevin Mitnick is one of the United States' most famous hackers. He was extremely proficient and started at the young age of twelve years old. He was charged with 14 counts of wire fraud, 8 counts of possession of unauthorized access devices, interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer (Brunker). Mitnick simply copied information he had gained access to and never profited from these intrusions. In a way, he acted as an advanced level security tester by exposing these flaws.

After committing this host of crimes, he was sentenced to an Internet-free life after serving his time in prison. He was unable to work with computers or computer-related equipment or software. This cut out almost any professional opportunity, he couldn't even obtain a fast food restaurant position because of computerized registers.

A hacker, Deric Lostutter, exposed school football members. In the video that was shown to the public, you can see a young woman get physically assaulted by these members of the football team. Lostutter was caught and received a sentence five times longer than the depicted rapists (CBS News). These crimes do not deserve outcomes with restrictions and limitations.

## **VI. Alternative Courses of Action such as Temporary Bans or Trials**

The intentions of these Hacktivists were positive, they risked their freedom to bring awareness to unethical and illegal activities. However, as punishment for using illegal methods to shed light, they will be banned from resources for the rest of their lives.

If convicted hackers are barred from accessing computers, being free is no different than being in prison. Alternatively, during their supervised releases, we recommend trials and temporary bans. The restrictions should be based on the severity of the crime committed. If the individual being tested fails to act in lawful and ethical ways, they may earn monitorization. After completing the specified period, they should be free.

Tommy DeVoss was convicted for hacking military banks and companies' websites in his early teens. He was put on juvenile probation and was banned from

accessing electronic devices until he turned 21. Despite this, he gained access to a computer. While he did nothing illegal with it, it went against the specified terms. He was caught after his probation officer made a surprise visit. DeVoss deconstructed his computer and hid the parts under his mattress, but he forgot to hide the mouse. He was sent to prison directly after this event.

After a man was convicted for distributing child pornography in his early 20's, he was still allowed to use the internet on cleared devices. He hacked the software and bypassed the program that tracked his browsing habits. Despite getting around this monitorization, authorities checked his hard drive and confirmed the violations of his terms. He too was sent to prison directly following this event (Murphy). These are both examples of the trials and bans working, when violators are caught they will face harsher repercussions.

Mitnick had a similar case to DeVoss. After his sentence was completed, he was banned from using computers. Authorities caught him hacking again and he went on the run. He served more time in prison following his capture. This second sentence involved eight months of solitary confinement because authorities believed he could use a simple payphone to commit crimes.

Following this sentence, he was once again banned from using any communications technology, but he fought this ruling through the appellate court system and regained internet access. He now runs a security consultancy firm and runs training sessions. By all accounts, he is a rehabilitated individual.

Ochoa has not been so lucky. He still works as a programmer. However, he has to write code without IntelliSense and physically print and mail his work to his supervisor. It's quite difficult to reintegrate with society when you don't have the resources any other individual is awarded upon release.

An individual that has been convicted for a sex crime must register as a sex offender. The severity of the crime determines the length they must be listed. In most cases, a registered sex offender that has served time in prison for possession of child pornography can still have access to a device with internet access. By all accounts their crime was aided by the use of the internet.



As a reference, there could be a registry for those who committed computer fraud and abuse. A judge can determine the length of time they must be listed by taking their behavior in prison into consideration. While registered, they will be monitored and have restricted access. By implementing this system, they will not be permanently punished.

## **VII. Supreme Court Decision**

In 2017, the United States Supreme Court issued a ruling declaring a North Carolina statute barring sexual offenders from “accessing a commercial social networking Web site where the sexual offender knows that the site permits minor children to become members or to create or maintain personal Web pages” (Supreme Court), as invalid, reversing the ruling of the North Carolina Supreme Court. This ruling is known as *Packingham v. North Carolina* and deals primarily with First Amendment rights. SCOTUS stated in its opinion that the Government may not suppress lawful speech as the means to suppress unlawful speech. While this ruling relates to the restrictions of previously convicted sexual offenders, it can be reasoned that the same logic could be applied to hackers, specifically black hat hackers that have been convicted of cybercrimes by the State.

The consequences of breaking certain statutes is similar, starting with the barring of certain Internet services. For clarification, this analysis focuses on convicted hackers being completely banned from Internet usage, even after their sentence has been served. While the outright ban of Internet services was not the case for *Packingham v. North Carolina*, it was found that the State had passed a law with such a wide breadth that it had expanded beyond that of what the State was trying to prevent. In *Packingham v. N.C.*, sexual offenses are what the State was trying to prevent in passing its initial legislation. Most repercussions for breaking the law try to prevent you from performing that illegal action. Therefore, one can assume that it is the State’s interest to prevent cybercrimes, especially those that target governmental entities, by banning convicted hackers from the internet. While it is already illegal ban people, we must consider the ethical implications of this SCOTUS decision from both a teleological and deontological point of view.

## VIII. Teleological Perspective

The first ethical perspective we are going to view this decision through is the teleological point of view. More specifically, we are going to focus on utilitarianism, which is the most common teleology approach (WPSU). Utilitarianism is a theory that aims to maximize the overall good for society as a whole, or in other terms, provide the greatest amount of utility for the greatest amount of people. To begin this analysis, one must look at the affected parties. The most prominent parties are the government, individuals (general public) who use the internet for various reasons such as shopping, education, communication, etc., companies, specifically high profile and financial institutions, and the hackers themselves (Pew Research Center).

The government has much to lose in this situation. Sensitive data, essential systems, and money due to ransomware are at risk if they are to be hacked by bad actors. In this analysis, we assume that the bad actors have already committed the crime, been convicted, and served out their sentence. By serving this sentence, the criminal has gone through the criminal justice system and should have been rehabilitated if the system worked the way it was designed to. By adding in this provision of banning internet access, it effectively extends the punishment and prevents ex-criminals from re-entering society. But from a government perspective, this measure is preventative and necessary. Therefore, we can conclude that the government gains utility because they are preventing people from attacking them.

Individuals, on a large societal scale, are at risk of attack all the time, whether it be identity fraud, financial loss, etc. *Figure 1* describes the amount of complaints the FCC receives from consumers (III). It must be noted, however, that this graph does not explicitly state whether hacking, forms of social engineering, etc. are the main cause of the complaint. Regardless, consumers are regularly targeted by attackers. If these convicted criminals, regardless of who their original victim was, are banned from the internet then it goes to say consumers would gain utility. This utility, however, is relatively small due to the sheer number of attacks that occur. Every complaint does not result in a conviction, or even as case for that matter.

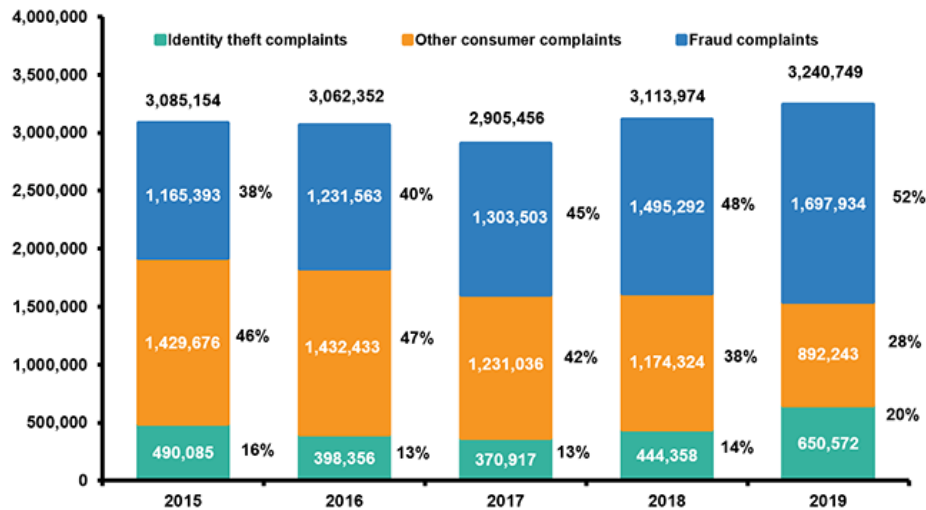


Figure 1

The last prominent party to analyze is the hackers themselves. Hackers are the most affected by the decision of the government as the consequences directly relate to their individual lives and how they can act. By banning these convicted hackers, the government is effectively cutting them off from society. They would not be able to communicate as effectively or educate and entertain themselves. In addition, it would be less likely that they could commit cybercrimes again. This fact is why these laws are passed to begin with. Since convicted cybercriminals are small in number compared to the amount of people who use the internet, the utility that they lose from the ban is smaller compared to that utility the government and internet users receive from the outright ban.

From a teleological point of view, after taking in the perspectives and gains/losses from the affected parties, we can conclude that this SCOTUS *Packingham v North Carolina* decision is unethical because it rules against the government and individual users and instead rules in favor of the criminal. Since teleological perspective forces us to consider consequences on a societal scale rather than individually, we can see that society gains the most benefit from convicted hackers being banned due to the risk that is mitigated. The government seeks to protect its data and internet users want a secure and safe environment to use the internet. While the internet is never safe, it can be concluded that banning hackers from the internet does, to some extent, prevent these criminals from committing cybercrimes again.

## IX. Deontological Perspective

The second perspective we are going to view this decision through is the deontological point of view. This perspective is much different from the teleological point of view in that it does not consider consequences. Instead, deontology focuses on individual rights (duties) and obligations. Individuals can have either perfect or imperfect duties. Perfect duties must always be honored, whereas imperfect duties have flexibility in deciding how and when to obey them. In addition, deontology focuses on our intentions rather than the consequences of our actions. We can control our intentions and change them if we want whereas consequences are out of our control and cannot always be accurately predicted.

Referring back to the 2017 SCOTUS decision, it is evident that this case involves fundamental rights that we have as humans. The fundamental right in question is the right to freedom of speech, guaranteed by the First Amendment of the Constitution. Another in question is the Right to Know. The internet is a platform where users can express themselves in addition to learning and exploring the world and people around them (Pew Research Center). Given this fact, it is reasonable to conclude that the rights in question are being violated by an outright ban on the internet.

In this analysis, we must determine whether these rights are imperfect or perfect. The right to free speech can be seen as imperfect because the State can limit speech to a certain extent, though it may not be by much. An example of limitations on free speech would be that people are not allowed to incite actions that would harm others. Right to Know can also be seen as imperfect due to the fact that the government can restrict certain documents and intelligence from the public. However, in this Supreme Court case, the Freedom of Speech (i.e. expression) that is being limited through the internet ban is protected because it is not presenting a danger. Moreover, the Right to Know is protected because classified information is not at stake, instead we are focusing on knowledge in the public realm.

Since deontology states that the ethical stance of an issue depends on the rights of the individual, we can conclude that the Supreme Court decision was ethical. The right to free speech is prevented through an internet ban because people would not be able to express their opinions in such an openly public domain and they would

not be allowed to communicate in a manner consistent with the modern age. The Right to Know is prevented because the internet by definition is an interconnected set of webpages that contain data and information. If this data is inaccessible due to the force of the State, it is unlawful and unethical. Therefore, the State, under this perspective, is not allowed to abridge these rights, even for its own interests.

## **X. Normative Recommendation for the Ethical Dilemma**

Our normative recommendation is that those banned from using the internet appeal the decision. They should procure a legal defense to draft their appeal and begin litigation. Civil and criminal decisions of a court are subject to review by an appeals court. An appeals court determines what occurred in prior proceedings and searches for any errors of law. During an appeal, the court will accept the facts as they were presented during the original trial, unless the finding goes against evidence (Findlaw).

Societal stakeholders, especially the forgotten felons, will benefit from successful cases as they can be used as references or create new policies and laws as seen in *Packingham v. North Carolina*. Kevin Mitnick now works to protect those he once harmed. He is currently a paid security consultant on top of writing books and attending public speaking engagements. As a security consultant, he works for Fortune 500 companies and the FBI. He performs penetration testing and teaches Social Engineering classes to companies and government agencies (Encyclopedia.com). When skilled individuals can use their knowledge for good, everyone benefits.

There should be a larger emphasis on rehabilitation rather than punishment. Mitnick shouldn't have had to fight to prove that he was trustable. He should've been given that opportunity during his supervised release. Instead of being locked away and alone in solitary confinement, he should've received care and sessions to help him understand his talent, and why he was using it for the wrong reasons in the first place. His reentry into the world was stunted by a lack of access to his profession.

We cannot speak about rehabilitation without scratching the surface on prison reform itself. The current criminal justice system was created for the rehabilitation of

offenders, but it can be argued that it has lost its way. Punishments are dealt inconsistently, and the primary institutions such as the police and prisons are under fire. The US' recidivism rates are abysmal in comparison to other established countries. Over an eight-year period, the recidivism rate for non-violent offenders was almost 40% (Clarke). Felons are not receiving the support they need. Almost 45% of offenders were arrested within one year of their release (Clarke).

We understand that there are cases when it is undesirable for certain individuals to use the Internet. A common argument is that those guilty of sexual crimes involving minors should have their access revoked, but as we have seen from *Packingham v. North Carolina*, the US' official stance is that this would be a violation of their rights. There is a greater focus on rehabilitating individuals guilty of these crimes, but the same cannot be said for those guilty of cybercrimes.

When the system fails them, it is no wonder they behave in the same way once they are released. Convicted criminals should not be banned from using the Internet. They should be slowly reintroduced and complete trials to show the legal system that they are worthy of being upstanding citizens and regaining the basic rights they deserve. Since this is not the case, the decisions should be appealed.

## **XI. References**

- "Appealing a Court Decision or Judgment." *Findlaw*, 3 Apr. 2019, [litigation.findlaw.com/filing-a-lawsuit/appealing-a-court-decision-or-judgment.html#:~:text=Most civil and criminal decisions,for any errors of law](http://litigation.findlaw.com/filing-a-lawsuit/appealing-a-court-decision-or-judgment.html#:~:text=Most civil and criminal decisions,for any errors of law).
- Bertrand, Natasha. "A Former Hacker Describes How He Survives Being Banned from the Internet." *Business Insider*, 27 Apr. 2015, [www.businessinsider.com/a-former-hacker-describes-how-he-survives-being-banned-from-the-internet-2015-4](http://www.businessinsider.com/a-former-hacker-describes-how-he-survives-being-banned-from-the-internet-2015-4).
- Brunker, Mike. "Mitnick Goes Free, but Must Remain Totally Unplugged." *NBCNews.com*, NBCUniversal News Group, 28 Apr. 2000, [www.nbcnews.com/id/3078786](http://www.nbcnews.com/id/3078786).
- Clarke, Matthew. "Long-Term Recidivism Studies Show High Arrest Rates." *Prison*

- Legal News*, 3 May 2019, [www.prisonlegalnews.org/news/2019/may/3/long-term-recidivism-studies-show-high-arrest-rates/](http://www.prisonlegalnews.org/news/2019/may/3/long-term-recidivism-studies-show-high-arrest-rates/).
- Clement, J. "Internet Users by Global Regions 2019." *Statista*, 14 Feb. 2020, [www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/](http://www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/).
- Clement, J. "U.S. Online Shopping Order Value by Device 2019." *Statista*, 27 Mar. 2020, [www.statista.com/statistics/439516/us-online-shopping-order-values-by-device/](http://www.statista.com/statistics/439516/us-online-shopping-order-values-by-device/).
- Davis, Don, et al. "US Ecommerce Sales Grow 14.9% in 2019." *Digital Commerce 360*, 9 Mar. 2020, [www.digitalcommerce360.com/article/us-ecommerce-sales/](http://www.digitalcommerce360.com/article/us-ecommerce-sales/).
- "Demographics of Internet and Home Broadband Usage in the United States." *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 12 June 2019, [www.pewresearch.org/internet/fact-sheet/internet-broadband/](http://www.pewresearch.org/internet/fact-sheet/internet-broadband/).
- "Facts Statistics: Identity Theft and Cybercrime." *Insurance Information Institute*, [www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime](http://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime).
- "Hacker Who Called Attention to Ohio Rape Case Facing Charges." *CBS News*, CBS Interactive, 12 July 2016, [www.cbsnews.com/news/steubenville-ohio-hacker-kyanonymous-who-called-attention-to-rape-case-facing-charges/](http://www.cbsnews.com/news/steubenville-ohio-hacker-kyanonymous-who-called-attention-to-rape-case-facing-charges/).
- "Kevin Mitnick Case: 1999." *Encyclopedia.com*, 3 July 2020, [www.encyclopedia.com/law/law-magazines/kevin-mitnick-case-1999](http://www.encyclopedia.com/law/law-magazines/kevin-mitnick-case-1999).
- Kurbalija, Jovan. "Virtual Sovereignty: Governments, Stakeholders and Internet Governance." *World Politics Review*, 11 Mar. 2014, [www.worldpoliticsreview.com/articles/13619/virtual-sovereignty-governments-stakeholders-and-internet-governance](http://www.worldpoliticsreview.com/articles/13619/virtual-sovereignty-governments-stakeholders-and-internet-governance).
- Murphy, Heather. "How Convicts Ordered to Stay Offline Try to Slip Their Digital Leashes." *The New York Times*, 26 May 2019, [www.nytimes.com/2019/05/26/us/computer-internet-restrictions-probation.html](http://www.nytimes.com/2019/05/26/us/computer-internet-restrictions-probation.html).
- Supreme Court of the United States. *Packingham v. North Carolina*. Oct. 2016, [www.supremecourt.gov/opinions/16pdf/15-1194\\_0811.pdf](http://www.supremecourt.gov/opinions/16pdf/15-1194_0811.pdf).
- Sandle, Tim. "UN Thinks Internet Access Is a Human Right." *Business Insider*, 22

July 2016, [www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7#:~:text=Due to the lack of,/HRC/32/L](http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7#:~:text=Due to the lack of,/HRC/32/L).

“Stakeholder.” Stakeholder Dictionary Definition,  
[www.yourdictionary.com/stakeholder](http://www.yourdictionary.com/stakeholder).

“UN: Majority of World's Population Lacks Internet Access.” *UPI*, 18 Sept. 2017,  
[www.upi.com/Top\\_News/World-News/2017/09/18/UN-Majority-of-worlds-population-lacks-internet-access/6571505782626/#:~:text=Sept.,to a United Nation report.&text=Of the 7.6 billion people,percent, are using the internet](http://www.upi.com/Top_News/World-News/2017/09/18/UN-Majority-of-worlds-population-lacks-internet-access/6571505782626/#:~:text=Sept.,to a United Nation report.&text=Of the 7.6 billion people,percent, are using the internet).

Welsh, Albina. “How Internet Affected the Modern Educational Process.” *Education Beyond Borders*, 2 May 2018, 11:04, [www.educationbeyondborders.org/profiles/blogs/how-internet-affected-the-modern-educational-process#:~:text=Modern education process has changed due to the use of the internet.&text=They use the internet to,where courses are done online](http://www.educationbeyondborders.org/profiles/blogs/how-internet-affected-the-modern-educational-process#:~:text=Modern education process has changed due to the use of the internet.&text=They use the internet to,where courses are done online).

WPSU - Penn State Public Media. Ethical Orientations: Teleology, The Arthur W. Page Center, [pagecentertraining.psu.edu/public-relations-ethics/core-ethical-principles/lesson-1-title/ethical-orientations-teleology/](http://pagecentertraining.psu.edu/public-relations-ethics/core-ethical-principles/lesson-1-title/ethical-orientations-teleology/).