High School Year 3: Government, Privacy, & You

Debates, A Riveting Play, Group Activities, & More!

Suggested use class-time: 5 Periods

Topics: Constitutional rights, privacy law & policy, debating privacy vs. security, and critical thinking skill development.

Worth noting: Teaches students about their constitutional rights by exploring the history of Edward Snowden's national intelligence leaks. Now, a new play about privacy is available to truly bring this material to life for your students!

For more information or to request a resource, contact our Senior Director at
mkamer@projectrealnv.org or 702.703.6529

Or visit:
http://projectrealnv.org

Project REAL's "The Government, Privacy, and You" Teacher's Guide

5 DAY SUGGESTED USE

Through your participation in *The Government, Privacy, and You,* you are offering your students an opportunity to gain knowledge and develop opinions about privacy. We rely on you to share the concepts and materials necessary for your students to understand how privacy laws can affect them. This Teacher's Guide has been created to help you and your students throughout this exciting opportunity, remember to choose the activities that fit your needs best. Thank you and enjoy!

DAY 0 – Friday: PREPARING YOUR STUDENTS FOR THE *GOVERNMENT, PRIVACY, AND YOU EXPERIENCE*

Before handing out the guidebooks, have your students complete the pre-test: http://bit.ly/privacypretest
Distribute the guidebooks and hold a general discussion, asking what the students know about Edward Snowden.
If they're uninterested, pull one of the articles from the app, summarize it, and ask students their opinions about the story.

ASSIGNMENT: Students should read pages 1-5 and write a brief paragraph explaining which 'Theme' of privacy concerns them the most and why they find it so concerning.

DAY 1 – Monday: Intro to Privacy Themes & Concepts

Discuss the reading assignment with your students (using the group discussion Q's on pg. 5 if you wish)
Read cases 1, 3, & 5 (pgs 21-24), discuss the questions with each case, & look to the table (32-38)& see how each case was decided

ASSIGNMENT: Have the students read pgs. 6-13 as homework. If you're up for grading material, ask them write a brief essay that e plains which surveillance program and which privacy-related law seemed the most important for them to know about, and why it was important to know those things.

DAY 2 – Tuesday: Snowden Reviewed

Discuss for up to 15 minutes what they thought of Snowden, his actions, and the governments work
Spend ten minutes discussing privacy vs security
Review as a class Pages 14-17, engaging in conversation using the questions listed at the end of each theme.

ASSIGNMENT: Write ½ a page: What does the constitution value more: Privacy or Security, and what laws make you think that?
A**SSIGNMENT 2:** Break the students up into 3 groups (defense, prosecution, judges). Each group needs to read pages 20-21, and be prepared to quickly follow the instructions for their side when class starts the next day.

DAY 3 – Wednesday: Mock Trial

Open with a VERY BASIC review on how legal-precedent works (ask us if you need a refresher).
Group Activity, "Edward Snowden: Guilty or Innocent?"
Have the students follow instructions on page 20 & get to the group activity "Edward Snowden: Guilty or Innocent?"
Discuss the outcome of the mock trial and reflect on what could have happened in order to result in a different outcome.
If you run out of time, save this for FRIDAY (Try not to run out of time).

ASSIGNMENT: Give students the option to watch '**A Teen's Home is Their Castle' at http://bit.ly/realprivacy2018**

DAY 4 – Thursday: THIS STUFF AFFECTS YOU.

Discuss what happened in the play & what your students thought the outcome of Parker's actions would be Vs. how the play ended
Would you have known how to exercise your rights that just because you have rights doesn't mean you get out of punishment?
How does this play apply to privacy? What did they learn? How important is understanding your rights and how to use them?
How does this apply to what was learned about Edward Snowden?
Who's opinions changed about Snowden after seeing the play? Who's opinions changed about enforcing laws vs right to privacy?
Explain how and why.

ASSIGNMENT: Have students write an essay about how their views have changed since the start of the week.

DAY 5 – Friday CONCLUDING *THE GOVERNMENT, PRIVACY, AND YOU* **(DAY 5)**

Have students complete the Post-tests after the final discussion found here (link will be provided to you: http://bit.ly/privacyposttest Have a class discussion about what constitutional rights the students have, know how to exercise, or want to learn more about. If possible, invite a guest speaker from Project REAL or the ACLU to close out the unit by answering students questions about the law & their rights.

Please make sure to have students complete the pre-test and post-test in order to help Project REAL determine how the program materials may be enhanced. There are also additional activities that are included in the guide if you choose to expand the lessons or assign extra credit. Remember that Project REAL allows for teachers to teach whatever they see fit on their own time. You can choose to focus on The Government, Privacy, and You for an entire week, every other day, or for five Fridays. It's all up to you!

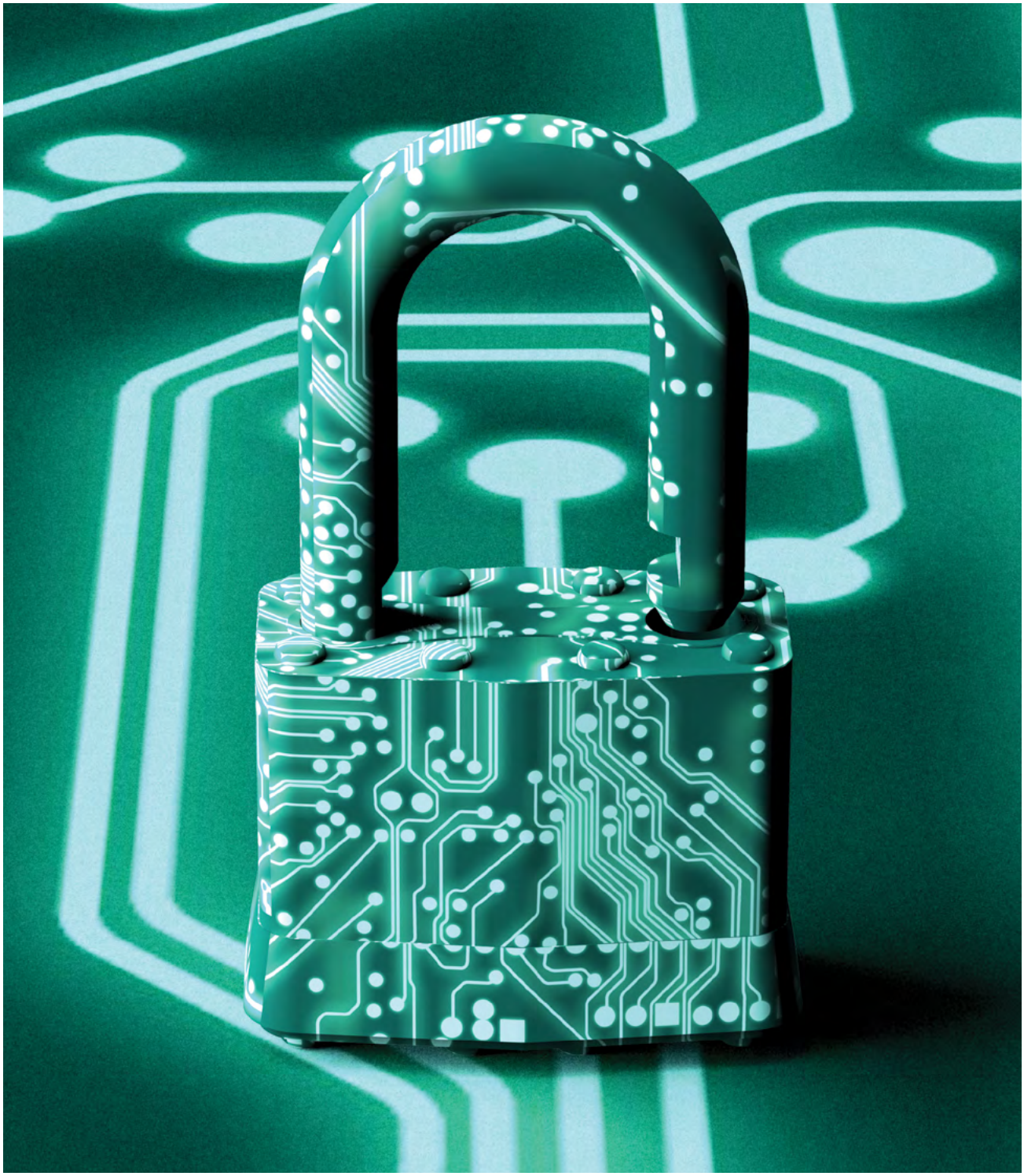
PROJECT real

GOVERNMENT, PRIVACY, & YOU

Student Guide

Table of Contents

I – PRIVACY



Goals

The Government, Privacy and You

You've grown up in a world of exponential improvements in technology, heightened national security, and wars being waged in manners unlike anything in human history – where information can be the greatest weapon of all. As a result of this world – your world – the issue of privacy has never been so complex and relevant. There is little agreement around the definition of privacy. Does it refer to being left alone? Is it about secrecy? Is it both?

This book highlights just a few of the many problems that result when privacy and law meet. Privacy is at the center of constitutional debate, legal action, legislative arguments, development of school district policy, and conversations in homes across the nation. You will be given the opportunity to not only form your own opinions about privacy, but to craft strong factually-supported arguments to support those opinions. Additionally, your instructor may choose to show you a short play about a case involving privacy law in the state of Nevada, so you can see how privacy laws have affected students just like you.

As You Read

As you make your way through this book, you may notice **words in bold red**. These are vocabulary words you may not be familiar with. When you see these words, use the glossary in the back of the book to learn their definitions.

How Should This Text Impact You?

Neither the book, the activities, nor the presentation are meant to tell you what to think about privacy or privacy law. These materials were created to help you develop your own thoughts and opinions about privacy. The issue of privacy law is an issue with no clear answer; however, after studying the subject:

- You should be able to explain and debate the concept of privacy in an informed and relevant manner and know several legal terms related to privacy law and policy;
- You should have a clear understanding of the importance of privacy in your life, the impact of privacy laws on your life, and why it is important for you to protect your own privacy;
- You should begin developing your own feelings and thoughts about privacy while recognizing that as the issues involving privacy continue to evolve, your views and feelings about it may change as well; and,
- You should find yourself thinking about how you might work to shape privacy law and policies in your community.

Privacy Concepts & Themes

What is Privacy?

In December 1890, future Supreme Court Justice Louis Brandeis defined **privacy** simply as the right "to be let alone." Professor Ruth Gavison summed up privacy with three words: "Secrecy, anonymity and solitude." Charles Bahmueller wrote that there are two types of privacy: "The right to keep something from being known to others…and the right to stop others from intruding upon something that is private." Another definition of privacy is the right to be secure against unlawful governmental intrusions. In the following years, that definition has grown to mean that privacy is the right to keep secrets from others as well as the right to keep anyone from intruding into your private space.

A major hurdle in reaching a clear definition of privacy is that the law has been unable to keep up with the rapid developments in technology. The age of instant online information challenges and reshapes privacy law and **policy** almost on a daily basis. As far back as 1890, Justice Brandeis asserted that technology challenged our definition of privacy, "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual…the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" Brandeis could scarcely have imagined the speed with which "the sacred precincts of private and domestic life" could be spread on the internet. Clearly, the issue of privacy has become even more complicated with the expansion of technology.

P 1.a) *How would you define personal privacy?*

P 1.b) *What does the word privacy mean to you?*

1.c) *Is it the responsibility of the government to protect your privacy? Explain your answer.*

1.d) *Should there be laws to protect your privacy? Explain your answer.*

1.e) *In what ways has technology changed the amount of privacy you have?*

What is Not Private?

As important as it is to understand legal privacy rights, we must understand where those rights end. In certain situations and locations, our privacy rights are limited. Whether we like it or not, it is possible for the government, our neighbors, friends and even strangers to know private things about us. This includes where we shop, the routes we drive, the physical location and description of our homes, where we bank, the restaurants we frequent, who our friends are, and more, through the cameras that are now placed throughout our communities, the use of satellites, cell phones, and internet sites.

The definition of privacy sounds simple enough, doesn't it? What is your private space – your room, your diary, your house, your locker, your backpack, your computer, your cell phone? Not anymore. Under certain circumstances, most often with a **warrant**, law enforcement or school officials have access to all of those things. It is important for you to know that under the law, students, employees, prisoners, immigrants, and even celebrities have specific limits on what is and is not private.

For example, police officers can seek a warrant signed by a judge granting them permission to search for specific items in your home, such as your computer or your cell phone. Remember that in a school setting, with only **reasonable suspicion**, school administrators may search your locker, backpack and/or purse.

Ronald Standler explains in his 1997 essay, Privacy Law in the USA, that "there is no protection for information that either is a matter of public record or that the victim voluntarily disclosed in a public place." In this technological age, information access has greatly expanded with large parts of the internet now considered a "public place." Blogs, social networking sites, YouTube, etc. are all considered public spaces despite the fact that we often access those sites from the privacy of our homes.*

*Read about Moreno v. Hanford (Case 9, page 26) to get deeper insight into what the law considers public and private.

Edward Snowden, The Modern Era of Privacy and You

The New Privacy Paradigm

You live in a world dramatically changed by the events of September 11, 2001. For example, new security policies were quickly put into place across the world in late 2001 in response to the attacks. These policies were referred to as **heightened security** processes and were only meant to be used in times of imminent threat or emergency. By 2005, many of the 'heightened security' policies had become security **norms**. The things people did during what used to be called 'times of heightened security' are now things we do on a daily basis without a second thought.

The shift in security standards is what some would call a **paradigm** shift, since changes to standard practices from what they once were have now become rules that we live by. This is an important concept to understand because another paradigm shift is happening now – a shift to a new privacy paradigm. The new privacy paradigm will affect how privacy is treated and dealt with for many years to come. Both the privacy and security shifts were the products of the 9/11 terrorist attacks. Unlike the changes to security however, the effects the September 11th attacks had on privacy went unnoticed for more than 11 years.

A Brief History of the Edward Snowden Leaks

On June 5, 2013, it became clear that the world had changed forever, and soon after it would be revealed that this change was brought about by one person – Edward Snowden.

Edward Snowden is a former Central Intelligence Agency (CIA) employee and National Security Agency (NSA) contractor. With a background in digital security, Snowden began working for the CIA as a computer technologist in 2006 and remained there until 2009. After his time with the CIA, he began work for Dell, a private company that provided services to the NSA. While the CIA and NSA's private contract partners do not have full access to national security systems, they are given access to systems related directly to the work they provide.

Photo by Laura Poitras / Praxis Films

Throughout his work at the CIA and with Dell, Snowden had learned about a number of intelligence programs and activities that he believed violated **constitutional law**. Snowden sent numerous emails and held many conversations with his superiors to report those concerns, only to be ignored or quickly dismissed each time. In some instances, he was even told to 'stay silent.' Frustrated with his lack of progress, in December 2012 Snowden began reaching out to journalists whom he thought of as trustworthy. At the same time, he began to collect documents he could use as evidence in case he did decide to come forward as a whistleblower. Hoping the concerns he reported might still be acted upon, Snowden put off revealing his identity to the journalists he contacted and withheld the documents he had collected to possibly use as evidence.

In March 2013, Director of National Intelligence James Clapper lied to the United States Senate Select Committee on Intelligence. Clapper was asked, "Does the NSA collect any type of data at all on millions, or hundreds of millions of Americans?" and he replied, "No Sir." When asked a second time, Clapper replied, "Not wittingly. There are cases where they could inadvertently, perhaps, collect, but not wittingly." The committee asked Clapper if the government had been engaged in activities that collected the data of American citizens, and Clapper had denied their existence. These were the very activities that Edward Snowden believed to be illegal surveilling Americans without **probable cause**. He had been trying to address his concerns internally, yet one of the heads of national security had just lied to members of the United States Senate to protect them. It was this incident that led Edward Snowden to take action.

Shortly after watching the testimony and feeling that he had no other choice, Snowden felt compelled to publicly expose the programs Clapper had lied about. The first step he took was to quit his job with Dell, so he could find work that would provide him with better opportunities to collect more evidence of the programs he planned to expose. Thanks to his experience working in the national intelligence field, he knew that contractors would have the best access to the records and evidence he would need. He sought positions with these agencies and quickly found work with Booz Allen (another **private contractor** that provided national intelligence services). Once there, he immediately began collecting evidence of activities that he thought were violating the **constitutional rights** of American citizens.

On June 5, 2013, Snowden began strategically leaking several documents that proved the United States government was spying on United States citizens. With the help of journalist Glen Greenwald and documentary filmmaker Laura Poitras, Snowden distributed different program records to reporters across the world. The reporters who received these records were then able to research and report on the leaked information for their newspapers. The choice to use different newspapers and reporters for each leak was made by Snowden, Greenwald, and Poitras as a way of guaranteeing at least some of the information would reach the public. The trio was concerned that the newspapers might be too scared of the consequences to publish the stories. They were also worried that the governments implicated by the leaks would directly interfere with their being published.

The first document to be released was a secret order from the **US Foreign Intelligence Surveillance Court** (**FISA**) that asked Verizon Communications to release metadata for all phone calls made in the United States and to other countries. In other words, the United States government had begun building a list of each American citizen's international friends and the friends of those international friends. The next release of documents exposed the NSA's PRISM surveillance program. This program allowed the NSA to access internet activity including web searches and e-mails being written in real time without a warrant. Over the next few weeks, Snowden helped expose even more surveillance programs being run by the United States government's security agencies. These programs were used to gather information on terrorist suspects, yet they were also being used to spy on American citizens and American allies. Once it was revealed that United States intelligence agencies were spying on the American people they were sworn to protect, the country was sent into a tail spin.

Because of Snowden, Greenwald, and Poitras' concerns about endangering national security while exposing the programs, it took news outlets months to report on the majority of the information that was being leaked. In fact, even three years after Snowden first leaked the documents, many of those documents have yet to be reviewed and reported on. While there is still plenty to be learned from the documents Edward Snowden leaked, one lesson was abundantly clear from the beginning: For over a decade, there had been two definitions of privacy in America – The one used by national security agencies working to protect the country, and the one known to the citizens of the United States.

Snowden and Your Thoughts and Feelings

Programs like Dishfire and XKeyscore allowed the government to see into people's private lives. Conversations weren't the only type of communication that could be intercepted. Poems, essays, stories, and journal entries could also be seen by the government, possibly without **due process of law**.

You may be familiar with the phrase "Life, Liberty, and the pursuit of Happiness" since it was used in the United States Declaration of Independence. This may come as a surprise, but the Declaration of Independence is not imbued with the same **legally binding** powers as the United States Constitution. The United States Supreme Court has occasionally used the Declaration of Independence to help interpret the **original intent** of the United States Constitution's authors. That being said, the content of the Declaration of Independence itself is not considered to be 'law.'

11.a) *Do you believe that it was the original intent of the Declaration of Independence's authors to imply privacy as a factor of 'Life, Liberty, and the pursuit of Happiness?' Why or why not?*

11.b) *Putting aside the original intent of the Declaration of Independence's authors, explain why you believe privacy is or is not implied by the phrase 'Life, Liberty, and the pursuit of Happiness.'*

11.c) *Putting aside the 4th and 5th Amendment protections that may be a factor, is there a greater need for programs like Dishfire and XKeyscore to examine people's private creative works (like stories, poems, essays, and journals)?*

11.d) *Do you think the government should use mass surveillance to look at people's private creative works as a way of finding people who have terrorist thought patterns? Remember – mass surveillance means everyone's private journals would be read – not just those of people already suspected of being terrorists.*

11.e) *If someone has expressed thoughts and feelings that suggest they are criminals or terrorists, but there is no other evidence against the individual, are those expressions a valid reason for authorizing highly invasive investigations?*

11.f) *Would those investigations be a form of thought policing? Explain how you feel about the concept of thought policing, and why you feel that way.*

Snowden and The Buying and Selling of Information

The Snowden Leaks did not suggest the United State's government was selling the data it collected, but they did spark conversations about the sources of metadata and how that data should be handled. Using the data produced by one person's **information footprint**, analysts could create extensive profiles of that individual. While these techniques were certainly used by the government in **profiling** terrorists, the public debate about metadata and privacy turned towards the commercialization of these profiles and the information used to create them.

Many service providers (companies like Facebook and Google) had begun selling their user data to marketing firms. These firms would create consumer profiles using that data, and then sell those profiles to businesses. The marketing companies claimed they were simply providing extensive market research, yet many consumers argued that their privacy was being invaded and manipulated. Allegations made in a lawsuit filed against Facebook in January of 2014 helped illustrate how private metadata could be misused by corporations. The alleged marketing program worked like this:

> Suppose Jane is a sports fanatic who loves to play basketball and watch football. She has 3,000 Facebook 'friends,' and naturally some of those friends also like sports. Jane shares her sports experiences through posts, and she regularly uses words like basketball or football in her writing. Facebook identifies her as someone who likes sports because of these posts and views her as valuable because of her 3,000 friends. Facebook then searches Jane's friends to see which of them also like sports. Nike would then pay Facebook for an ad to appear to Jane's friends. To her friends it would appear that Jane had 'liked' a new pair of shoes Nike was releasing, yet Jane might have never even heard of the shoes. Without her consent, Jane and her information would be used to endorse Nike's new product. Even if Jane disliked every Nike product she had ever encountered, she could still be used to endorse the company's new product.

Whether or not the allegations were true, the plausibility that metadata could be misused in this way certainly exists. Some lawyers might even argue this is an example of **tort** or an example of commercial **libel** and possibly even **slander**. Many mobile apps require users to agree to lengthy 'Terms of Use' agreements before gaining access to the programs, yet studies suggest few people read these agreements. Companies are certainly known for having users waive certain privacy rights by hiding waivers in their service term agreements. Apple and Facebook are notorious for their lengthy Terms of Use statements and the phone security permissions users are required to provide before being able to access the company's apps. Whether or not privacy violations actually happen, there is clearly a path for metadata misuse laid out by these conditions.

12.a) *If the marketing program Facebook was accused of operating was real, why do you think it should or should not be considered a violation of people's privacy?*

12.b) *What are some of the concerns you have about how companies could use your data?*

12.c) *Do you use apps and programs even though you have concerns about how your data will be accessed or used by the companies who've made those apps? Why or why not?*

12.d) *What laws entitle people to have their metadata remain private, if any?*

12.e) *Having learned about the many ways data can be used to invade your privacy, what behaviors (if any) are you thinking about adopting to protect your information? What are your reasons for protecting or ignoring the privacy of your information?*

II – ACTIVITIES

Privacy Law in Nevada (A brief presentation)

You will now either be shown a short film or asked to read the script. The subject of

this script is the roles privacy laws and policies play in your lives.

The story is about high school student here in Nevada who is rumored to have sent inappropriate photos of themselves to a friend.

The principal finds out about the rumor, and takes the student's phone.

The student then exercises then rights by refusing to unlock the phone at the insistence of the principal.

The principal issues an ultimatum: Unlimited detention until the phone is unlocked. We'll let you discover what happens next.

As you watch the presentation, think about the ways in which you are already familiar with the concept of privacy and the laws that apply to it. In studying privacy as an academic subject, you have:

- Learned basic concepts of privacy.
- Come to understand some of the ways in which privacy can be violated.
- Researched laws relating to privacy.
- Crafted arguments for and against activities which affected privacy.
- Used existing laws about privacy to support your arguments.
- Identified aspects of your life where the security of your privacy may be at risk.
- Developed a position on the conflict between privacy and security.
- Examined your values in the context of your own privacy and the privacy of others.
- Discovered some ways in which policies can be changed.

After the presentation, be prepared to answer the following questions:

- Which of the Five Themes of Privacy Issues were useful for identifying privacy issues in the presentation? Explain how the themes you've identified helped to present the case in the context of privacy issues.
- The presentation cited a few laws that were used to determine the outcome of the case. What other laws or legal precedents would you like to have seen applied to the case, and why?
- If you agree with the outcome of the case, what additional arguments would you make to support the outcome or what laws would you cite? If you disagree with the outcome of the case, what laws support your opinion?
- Edward Snowden risked his freedom by apparently breaking the law in order to stop privacy violations from occurring. Groups like the ACLU, Privacy Coalition, and the tech companies work within the legal system to change privacy policies and laws. Having watched the presentation, what policy would you create in response to the case you've learned about? Create a detailed plan for turning your policy proposal into rule or law.

GROUP ACTIVITY

Edward Snowden: Guilty or Innocent?

Applying What You've Learned

Have you ever thought about becoming a lawyer, a judge, or a politician? The previous section provided you with opportunities to use the law to support and defend your opinions. In answering those questions, you had a small sample of the kind of work people with those jobs do. In those careers, many of the greatest successes are achieved by people who learn to anticipate and prepare for the choices that will be made by their opponents. Now you have the opportunity to apply that type of thinking to your opinions.

Setting: Edward Snowden After The Leaks

Soon after Edward Snowden began releasing the information he had obtained, he made his way to Russia. Once he arrived, he requested **asylum**. This meant Snowden had asked Russia to protect him from being prosecuted by the United States. Russia granted his request, and eventually Snowden became an American citizen with Russian residency. Having been granted residency by Russia meant that he would be protected from **extradition** to America by the Russian government.

In June of 2013, Federal Prosecutors in the United States filed a criminal complaint against Edward Snowden. Because Snowden had been given Russian asylum, the United States was unable to bring him back to the country to be put on trial.

Federal prosecutors filed three charges against Snowden. The prosecutors argued Snowden violated at least three laws that were established by the 1917 Espionage Act. The charges were:

- Theft of government property (18 USC § 641),
- Unauthorized communication of national defense information (18 USC § 793(d), and
- Willful communication of classified communications intelligence information to an unauthorized person (18 USC § 798(a)(3).

Scenario: Edward Snowden on Trial

Suppose the following: Imagine it is the year 2022 and Edward Snowden has been successfully extradited to the United States. He was put on trial and found guilty. His lawyers appealed the decision that was granted, however, they lost on appeal. They appealed again, this time to the Supreme Court. The court has agreed to hear Snowden's Case.

Snowden's lawyers argue that the charges against him were misinterpreted. Snowden has stated on many occasions that he acted to protect the country, not to work against it. They argue that the espionage act was designed to prosecute spies, but that Snowden was being a patriot. They claim that not only should the charges against Snowden be dismissed because he did the right thing, but that the original intent of the law supports their claims.

The federal prosecutors (the original **plaintiffs** in the case) arguing the case see things differently. They claim that the laws under which Snowden was charged were clearly designed to protect secret government information from being released, regardless of the intent of the person releasing the information. From their standpoint, it is their duty to enforce all laws even when doing so might get in the way of justice, and that the stability of society relies on that kind of enforcement. They give the example of evidence collected without warrants. Even if some type of evidence proves undeniably that someone is guilty of a crime, if the evidence in question was collected without a warrant when a warrant was clearly required by law, then it is not allowed to be used in court.

A Quick Guide to Oral Arguments in The United States Supreme Court

When cases are examined by the Supreme Court, the justices first receive briefs – written arguments from each side about why the case should be decided in their favor. Next, each side is given a few minutes to address the court. After that, the justices of the court are allowed to ask questions. **Rebuttals** by the **appellate** are allowed if the appealing **party** sets time aside specifically to appeal. The **appellee** is not given the option of providing a rebuttal. The judges then go back and vote to see where they stand. Finally, they issue two opinions: the majority opinion that decides the outcome of the case, and the minority opinion that explains why some of the judges disagree with the final determination of the case.

Instructions

For the following exercise, your class will use the law to produce an informed hypothesis of how Edward Snowden's fate might be decided by the Supreme Court. Your instructor will break you up into three groups: There will be nine Supreme Court Justices, with the rest of the class divided into **Prosecutors** and **Defense Attorneys**.

- First, the prosecution and defense teams will each create a list of 3-6 laws they believe the opposing side will use against them. At the same time, each Supreme Court justice will work on their own to find 3 that support the lower courts in their decisions that found Snowden guilty. Whatever opinion you have going into the exercise, it is vital that you try to defeat yourself. Look for every law that supports the feelings of the opinion you disagree with. What support will they have? The more you find, the more you can be prepared to defend your position. During this time, the members of the Justice group will elect 1 member to be the Chief Justice.
- Next, the prosecution and defense teams will create a list of 3-6 laws that support their cause (defending or prosecuting Snowden). Once the list is ready, they will create a five minute presentation arguing their case that cites the laws they've used. Meanwhile, each **justice of the court** will work on their own to find three laws that support dismissing the charges against Snowden. Once the list is complete, each justice will come up with at least six questions to ask the attorneys; three for the prosecution and three for the defense. In this step, be sure to use the work from the first step of the exercise as you craft your arguments.
- 'Court' goes into session, with the appellant (Snowden's defense team) presenting first. After their presentation of 5 minutes or less, each justice may ask 1 question, which any member of the appellant team may respond to. The justices do not have to use the questions they prepared if they develop a different question as a result of the presentation they've heard.
- While Snowden's team is arguing and responding to questions, the appellee (the federal prosecutors) are encouraged to adjust their presentation as they see fit. When the justices have finished questioning Snowden's defense team, the prosecutors make their case, and again the justices each ask 1 question of the team. During this time, Snowden's team is allowed to prepare a 3 minute rebuttal.
- The defense team is provided 3 minutes to present their rebuttal. On behalf of the court, the Chief Justice may ask 2 questions about the rebuttal.
- During the next 15 minutes, the justices vote to determine the outcome of the case. Once the outcome is decided, they break up into 2 groups: those in favor of Snowden and those in favor of the prosecution. Each group crafts a 2-3 paragraph statement explaining how they arrived at their opinion. If a unanimous decision was reached, only 1 opinion statement should be written. While the justices are voting and crafting the court's response, the defense and prosecution teams will create a list of ten things they would do differently if they had a second chance to argue their case.
- The majority opinion is presented to the class, followed by the dissenting opinion. Next, one representative from each side will share the list of changes they would have made to their presentations.
- Finally, the class will discuss as a group if the proposed changes would have made a difference in the outcome of the case.

A Brief Note About This Exercise

This exercise presents a simplified version of actual Supreme Court procedures for oral arguments. The authors encourage you to take some initiative and read the transcript of the oral arguments presented in 'Department of Homeland Security V MacLean.' This was one of the first whistleblower cases to ever reach the United States Supreme Court. The transcript can be found here:
https://www.supremecourt.gov/oral_arguments/argument_transcripts/13-894_3c45.pdf

Reflecting on the Activity

13.a) *Think of the last time you were arguing an opinion outside of school. Using the methods you employed in this exercise, what would you have done differently to strengthen the case you were making?*

13.b) *Besides jobs in the legal and education fields, what other professions might use factual evidence to support opinions in situations where there is no clear answer?*

13.c) *In this activity, you were instructed to prepare counter-arguments without hearing what the opposing side had to say first. What are two ways you can use this skill that have nothing to do with writing school papers or arguing court cases?*

13.d) *What other lessons from this exercise will you begin using outside of the classroom, and how will you use them?*

Supplemental Cases and Statutes

This section contains 12 illustrations of how your private life and the law might interact. Read about each case, and consider the questions that follow them. Your teacher may ask you to write essay responses to some of the following questions, or may engage your class in group discussions about them. The final outcome of many of the following cases have not been included with this text in this section. While you could simply turn to the section 'A Historical Review of Privacy Law' to learn the final outcome of each case, the authors encourage you to first try and determine the outcome of the cases on your own. The cases are presented in this way so you have an opportunity to use the laws you've learned from the earlier portions of this book to make your case, rather than relying solely on your emotional viewpoints. By not knowing the final outcome of the cases, you are empowered to make educated guesses about what those outcomes were. As you review these cases, be prepared to explain which of the 5 themes of privacy they can be categorized under, and why you would categorize them that way. How you feel about privacy won't affect how efficient you will be as you argue for the privacy rights you believe you should have. Even in responding to questions that ask for your feelings and opinions, you should include factual evidence to strengthen the validity of your arguments. Thinking about privacy will not simply be a fun classroom exercise – as technology and privacy laws continue to change, you will have to consider your actions with increasing consequence in your life. By learning to craft and support your positions using factual evidence, you improve your ability to influence the outcome of policy discussions and developments. Look at how some legal circumstances have already affected the lives of people just like you.

Case 01

Katz v. United States (1967)

Summary: Charles Katz used a public pay phone booth to place illegal gambling wagers. Unbeknown to Katz, the FBI, without a warrant, recorded his conversations with an electronic eavesdropping device attached to the exterior of the phone booth. Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights.

Critical Thinking: Did Mr. Katz have a legal expectation of privacy when he was making a call from a corner phone booth, or did the FBI have the right to tap the phone of someone suspected in illegal practices?

Case 02

Nevada Revised Statute 202 (1967)

Summary: NRS. 202.020 Any person under 21 years of age who purchases any alcoholic beverage or any such person who consumes any alcoholic beverage…or possesses any alcoholic beverage in public is guilty of a misdemeanor.

NRS 202.2493 It is unlawful for any person to sell, distribute or offer to sell cigarettes, cigarette paper, tobacco of any description or products made from tobacco to any person under the age of 18. A person who violates this subsection shall be punished by a fine of not more than $500.

Critical Thinking: Do you think that whether or not you drink alcoholic beverages and smoke cigarettes is a private decision, one you should make without government interference? Do you think it is right for the government to make that decision for you? How do you feel about these two laws? Are they good for you and community?

Case 03
United States v. Ross (1982)

Summary: A reliable informant notified a detective that a man known as "Bandit" was selling illegal drugs out of the trunk of his car. The informant gave detailed information of the appearance of both the car and "Bandit." Other detectives located the car and learned it belonged to Albert Ross who used the alias "Bandit." After observing the car for a while, the officers saw a man matching the description of "Bandit" enter the car and drive away. They then pulled the car over and asked Ross to get out. One of the officers found a pistol in the glove compartment and, in the trunk, a brown paper bag filled with small bags of powder, $3200, and traces of another powder that the police lab later determined was heroin. No warrant was obtained.

Critical Thinking: Do you think the police had the right to search the car when their probable cause was solely based on information from an informant? If you agree, does that mean that if you told school or police authorities that a student at your school was selling drugs out of his car they would have the right to search it?

Case 04
New Jersey v. T.L.O. (1985)

Summary: In this case, a teacher in New Jersey suspected a high school student of smoking in the bathroom. The school's vice-principal was brought in and searched the student's purse looking for cigarettes. During the search, the Vice-Principal found marijuana in her purse, along with items that would indicate that the student was also selling marijuana. The student's attorney protested the search, believing that the Vice-Principal was required to have a warrant and that the search was a violation of T.L.O.'s Fourth Amendment rights.

Critical Thinking: Was the student treated fairly? Do you think students should have the same Fourth Amendment protections as adults? What would you guess to be the decision given by the Court? This case is considered a landmark case in determining the privacy of students. Why?

III – RESOURCES

Charges Against Snowden

18 U.S. Code § 641

Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted – Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of $1,000, he shall be fined under this title or imprisoned not more than one year, or both. The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

18 U.S. Code § 793

Gathering, transmitting or losing defense information

a. Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

b. Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

c. Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

d. Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated,

A Historical Review of Privacy Law

Date	Legislation / Case	Summary
1787	United States Constitution s.110, Article III	Treason against the United States shall consist only in levying war against them, or in adhering to their enemies, giving them aid and comfort. No person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open Court. The Congress shall have power to declare the punishment of treason.
1790	Act of April 30, 1790	If any person or persons owing allegiance to the United States of America, shall levy war against them, or shall adhere to their enemies, giving them aid and comfort within the United States, or elsewhere, and shall be thereof convicted on confession in open Court, or on the testimony of two witnesses to the same overt act of the treason whereof he or they shall stand indicted, such person or persons shall be adjudged guilty of treason against the United States, and SHALL SUFFER DEATH; and that if any person or persons, having knowledge of the commission of any of the treasons aforesaid, shall conceal, and not, as soon as may be, disclose and make known the same to the President of the United States, or some one of the Judges thereof, or to the President or Governor of a particular State, or some one of the Judges or Justices thereof, such person or persons, on conviction, shall be adjudged guilty of misprision of treason, and shall be imprisoned not exceeding seven years, and fined not exceeding one thousand dollars.
1791	1st Amendment	Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.
1791	3rd Amendment	No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.
1791	4th Amendment	The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
1791	5th Amendment	No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb, nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Date	Legislation / Case	Summary
1791	9th Amendment	The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people.
1791	10th Amendment	The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.
1868	14th Amendment (Section 1)	All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law that shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.
1925	Carroll v. United States	The Supreme Court held that federal agents had been justified in a warrantless search of an automobile that they had stopped on a public highway. The agents had probable cause to believe that it contained contraband. The Court found that the search had been justified, noting that, unlike a structure, an automobile can be "quickly moved out of the locality or jurisdiction in which the warrant must be sought."
1917	The Espionage Act	The Espionage Act of 1917 made it a crime to 'convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies, or to convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to willfully obstruct the recruiting or enlistment service of the United States.'
1928	Olmstead v. United States	This case addressed the issue of whether or not the use of a telephone wiretap could be excluded from evidence in a criminal trial. The Court ruled that governments could place wiretaps as long as governmental agents did not physically trespass when placing the taps (ABC-CLIO). This was the first time the Court heard a case about electronic technology.
1965	Griswold v. Connecticut	Declared unconstitutional a law that prohibited the use and distribution of contraceptives. This case was considered to be the first in which privacy was named an independent right, one found in the "penumbras" or shadows of the Constitution. Justice Douglas wrote that it was an invasion of the "zone of privacy." This case is still considered one of the most controversial in the Supreme Court's history.

Glossary

Air gapped computer – A computer that has never been connected to a network. This includes private networks, and public ones like the internet. These may also be referred to as 'air-gapped computer(s).'

Appellant – The party requesting a higher court to reverse the decision of a lower court.

Appellee – The party defending a lower court's decision from being reversed by a higher court.

Asylum – Protection provided by a nation to a political refugee fleeing their home country.

Civil law – Resolves non-criminal disputes such as disagreements over the meaning of contracts, property ownership, divorce, child custody, and personal and property damage.

Common law – Laws established through earlier judicial decisions (or precedents). In making their rulings, judges often rely on courtroom decisions from prior cases.

Constitutional law – Laws set forth in the Constitution of the United States and states' constitutions.

Constitutional rights – Legal rights that are provided to citizens by their nation's constitution.

Criminal risk assessments – Personality tests used to determine the likelihood of the test-taker committing a crime.

Damages – Monetary compensation that is awarded by a court in a civil action to an individual or party who has been injured through the wrongful conduct of another party.

Defendant – In criminal cases, the person accused of a crime; in civil matters, the person being sued.

Defense attorney – The lawyer serving on behalf of the party who has had a charge or accusation made against them.

Dissenting opinion – An opinion in a legal case that explains why the author disagrees with the final outcome of the case.

Due process of law – A fundamental constitutional guarantee that all legal proceedings will be fair. It also guarantees that one will be given notice of any proceedings as well as an opportunity to be heard before the government acts to take away one's life, liberty, or property.

Encryption – A security technique for sending communications that only the author and intended recipient are able to view.

ex: Using encrypted email, Annie sent a poem she wrote to Abed. She used encryption because she didn't know if the poem was good, and she wanted to get Abed's opinion before showing it to other people. When Troy found Abed's phone in the cafeteria, he was unable to open Annie's email. Only Abed and Annie had the password to decrypt the email, so only they could read it.

Espionage – The act or practice of obtaining secrets from competitors or enemies through spying /spy-craft.

Extradition – The act of passing custody of a person from one authority to another, usually as a result of criminal charges in the receiving authority's jurisdiction.

ex: Having arrived in Mexico, Vincent thought he had gotten away with robbing that bank in Texas. Shortly after however, Texan authorities contacted the Mexican police when they received a tip about Vincent's location. Vincent was captured by the authorities in Mexico, and then extradited to Austin where he would face charges of armed robbery.

FISA – See US Foreign Intelligence Surveillance Court

Heightened security – A term used to collectively describe the additional practices and increased levels of activity that result from a known or suspected threat.

Information footprint – Data produced by an individual, with or without that individual's intent or consent to produce a record.

Justice of the court – A voting member of the United States Supreme Court.

Legal opinion – A written explanation of a court case ruling that lays out the rationale and legal principles for the ruling.

Legally binding – A term used to describe the legal powers or authority of legislation or decrees.

Legitimate expectations of privacy – Times when a person can anticipate having some form of privacy.

Libel – An untrue or malicious publication that damages a person's reputation.

Living document – A document that receives regular updates and alterations.

Malware – Software or programs that are intended to disrupt computer systems without the consent of the owner.

Majority opinion – A judicial opinion that sets forth the decision of the court and explains the rationale behind the court's decision.

Metadata – Information that helps to identify and describe other data.

National security apparatus – A term used to refer to the collective body of organizations that work to achieve national security, as well as the tools and methods they use.

Norm – Something that is usual, typical, or standard

ex: Saying hello to someone you know is a cultural norm.

Original intent – A theory in law that argues that when laws are being interpreted, the original intent of the laws' authors should be the standard by which the law is interpreted.

Paradigm – A paradigm is a recognizable pattern that guides activities or behaviors of a system. A dramatic shift in the way which things operate is therefore called a paradigm shift.

Parole – The release of a prisoner with certain conditions and restrictions.

Party – An entity (individual, organization, or government) who is directly involved in legal proceedings (i.e., plaintiffs, defendants etc.).

Plaintiff – A person who brings an action or lawsuit to a court of law.

Policy – A plan or course of action by a government, political party, or business, intended to influence and determine decisions and actions.

Precedent – A judicial decision that can be used for the basis of another decision of a similar type.

Privacy – Generally speaking, the restriction of access to information, where information can be (but is not limited to) thoughts, feelings, or facts.

Private contractor – A person or business that provides services to a company with specific contractual obligations and limitations, similar to but different than an employee.

Probable cause – A realistic belief that a crime has been committed, is currently being committed, or will be soon, and sufficient evidence to warrant an arrest or search and seizure. Probable cause has a stronger standard of evidence than reasonable suspicion and can lead to an arrest.

Profiling – The analysis of a person based on their personal characteristics, their actions, or some combination or the two.

Prosecutor – A lawyer who represents the law / the government in criminal cases.

Reasonable suspicion – A legal standard that a person might have been, is, or is about to be, engaged in criminal activity based upon specific facts or deductions that can be clearly explained. A police officer has the legal right to stop and ask a person questions under the lower standard of reasonable suspicion. The police officer may frisk a suspect or detain the suspect briefly but may only arrest if evidence is obtained to move to probable cause or a warrant is issued.

Rebuttal – A response to a statement that argues against the factuality of the statement being responded to.

Sentencing – The act of setting a punishment once a party is found to be guilty of a crime.

Servers – Computers built to hold and share information for and with other computers.

Slander – Untrue or malicious spoken words that damage the reputation of another.

Snowden Leaks, The – The collective sum of the information released to journalists around the world by Edward Snowden.

Tort – A non-criminal legal wrong for which a person can be sued in a civil court and could be required to pay financial damages. There are four major kinds of privacy torts: appropriation, false light, intrusion, or invasion of privacy and disclosure.

US Foreign Intelligence Surveillance Court (FISA Court) – Established by the Foreign Intelligence Surveillance Act of 1978, this court oversees warrants issued for surveillance of suspects within the United States.

User agreements – Contracts made between service providers and the people who use them. Users are required to acknowledge that they agree to the company's terms in order to use that company's services.

United States Supreme Court – The highest court in the judicial branch of the United States that has the authority to have the 'final say' on how laws are interpreted.

Warrant – A written order by an official of a court authorizing an officer to search in a specific place for specified objects and to seize them if found. The objects sought may be stolen goods or physical evidence of the commission of a crime or crimes (e.g., narcotics).

Warrantless searches – Searches conducted without a warrant first being issued.

Whistleblower – A person who reports illegal activity being conducted by an organization. Usually, the person is an employee of the organization or closely affiliated with it.

7175 Bermuda Rd.
Las Vegas, NV 89178

(702) 703 - 6529
projectrealnv.org

@projectrealnv @ProjectREALOrg @projectrealnv_