Title: We.thePeople: American Government and Cybersecurity

Length of Course: Full Year (2 semesters; 3 trimesters; 4 quarters)

Subject Area – Discipline: History/Social Science ("a") – Civics

UC Honors designation: Honors

CTE Sector: Information and Communication Technologies

CTE Pathway: All four pathways (See "Information Support and Services")

Grade Level(s): 9-12

Overview:

American Government and Cybersecurity is a history/social science course integrated with the four pathways of the Information and Communication Technologies (ICT) sector and the National Initiative for Cybersecurity Education (NICE) standards. The course prepares students to see where the field of cybersecurity intersects with the American Constitution and political system. To accomplish this goal, the course content explores the relationship between cybersecurity and government through five dimensions: historical, technological, legal, administrative, and ethical, and explores how those dimensions affect U.S. policy in regards to citizen privacy as well as Homeland Security issues.The content of government includes eight big ideas of units: 1) Our system of government and cyber security, 2) Executive branch, 3) Legislative branch, 4) Judicial branch, 5) Election process, 6) State government, 7) Civil responsibilities v. government responsibilities, and 8) Evolution of Democracy. Throughout the eight units, students conduct research, closely read and analyze complex texts, participate in policy debates, and compose research papers in which they synthesize their knowledge to design a government policy that addresses a critical cybersecurity issue. At the same time, students are provided a rigorous pathway to learn government and technical knowledge, communication, critical thinking, and problem solving skills that prepare them for further college, career, and civic readiness in the field of Information and Communication Technologies and American Government.

Course Content:

Unit 1: Our System of Government and Cyber Security

Throught the work of this unit students will gain foundational knowledge in the Constitution, and will use that as a framework for understanding the role and influence of the internet in a Democracy. This will prepare students for being able to later identify and interpret more specific privacy issues related to cybersecurity and the branches of the government. Utilizing knowledge of the political principles underlying the U.S. Constitution and the American political system, students examine the Enlightenment ideas that informed the foundation of the American democratic system and apply them to an analysis of the new and ever evolving online world. Students examine the works of the Enlightenment Philosophers who inspired America's founders and hypothesize how these thinkers would respond to our new virtual experience. Students also watch the movie *1984* in order to discuss the impact of technological trends on society and their implications to policy makers.

Unit 1: Key Assignments

1. Meeting of the Minds and Reflection Paper

Students read teacher selected excerpts from various Enlightenment Philosophers (such as Locke, Voltaire, Rousseau, and Montesquieu) in order to examine these philosophers ideas and how they influenced the government established in the United States by the authors of the Constitution. Students also examine one of the many scholarly articles written about the internet and democracy such as the following: http://mikeb.inta.gatech.edu/uploads/papers/internet.democ.pdf published in the *Bulletin of Science, Technology and Society*. After reading, students participate in a "meeting of the minds" discussion in small groups. Each student either represents one of the philosophers or an "internet expert." The internet expert should explain the online world and its key components to the philosophers and ask them questions about how their ideas on democracy would influence how the government should use and regulate the cyber world. Students will then write an individual reflection paper summarizing in 2-3 pages what they think each philosopher would say in regards to the use of the internet and conclude by examining what we can learn from these philosophers in the way we approach the internet as individual citizens.

2. Preamble Analysis Blog Post

The goals of the government of the United States of America are laid out in the Preamble to the Constitution. After students read the preamble to the Constitution and conduct research or read teacher provided articles on the role/impact of the internet in today's world, students will take each of the six goals of the Preamble ("in order to form a more perfect union, establish justice, etc") and create a blog post identifying and analyzing how these six principles apply to the virtual world and the role of government in the virtual world. As an optional extension, students should post their blog on a school or class discussion board and moderate a discussion on the topic in order to apply the ideas of being a good digital citizen as described in articles such as this one http://www.teachthought.com/technology/20-basic-rules-for-digital-citizenship/ from te@chthought.com.

3. Interpreting the Constitution Poster

Students read "Strict vs Loose Constructionism" at the following link: http://scotus.tribe.net/thread/0d2d6753-a0ba-4ca2-9441-8d51af1dc355.
After reading the article, students research actual Supreme Court privacy cases that are examples of strict and loose interpretations of the constitution. Possible cases for study could be The National Bank, Roe.v Wade, Griswold v Connecticut and Riley v. California.

Students create a poster, powerpoint or other kind of presentation using technology that identifies the key points of the article (or a similar article) and that defines strict and loose interpretations of the constitution as it relates to privacy using specific examples of Supreme Court cases that connect to each interpretation. Finally, in a written summary and analysis, students make a determination as to whether the trend in the cases examined leans towards a strict or loose interpretation of the constitution, using evidence from the case studies to support their conclusion. This assignment lays a foundation for understanding interpretation of the Constitution as it relates to privacy and cybersecurity.

4. Movie Analysis and Discussion

After watching the movie *1984*, students research and write an analysis answering questions such as the following, and then participate in a class discussion:

- ➔ What technological applications today have presented threats to the public as the threats in the movie?
- ➔ What laws are in place or missing to address cyber threats?
- ➔ What would be the obstacles to enforce or to pass such laws?

The assignment provides students a deeper understanding of government's role in protecting civil liberties, such as privacy, from the intrusion of technology, as well as government's potential abuse of power with technology.

Unit 2: The Executive Branch

After an exploration of the basic functions of the Executive Branch, students analyze the implications of cyber security technologies on the vast bureaucracy that forms this central branch of government. Students will explore many of the departments of the Executive Branch and explore the job requirements to get a job with the Executive Branch. Students will then debate the legality of Executive orders issued by the President in regard to cyber security.

Unit 2: Key Assignments

1. E-Government and Technology: Public Safety & Awareness Resource

This assignment is meant to help students explore and understand the various resources and programs that exist as a result of executive orders to help protect victims of cyber crime.The government has made cyber security a priority starting with the Comprehensive National Cybersecurity Initiative in 2009 which led to numerous executive orders. After instruction in the basic functions of the Executive branch, students learn about specific executive orders and the programs associated with them through examination of the following websites:
http://csrc.nist.gov/nice/awareness.html
http://www.stopthinkconnect.org
http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
https://www.ftc.gov

In order to synthesize the scattered and difficult to find information that a victim of a cyber crime might need to access, students create a resource (a video, a pamphlet, etc.) that would help someone navigate these programs and understand what is available to them through executive orders. This may include internet safety or how to protect people from internet scams. The students may also use this opportunity to identify overlap in government information. The outcome is a synthesis of cyber security information.

2. Working for the Government Pamphlet

The Executive Branch is the largest employer in the United States, and many jobs within the government require a background check or security clearance. Students will examine departments of the executive branch, such as the Department of Justice, and their purpose/role. The DOJ includes the Attorney General, FBI, ATF and others. In their investigation, students should examine the jobs, including cybersecurity jobs that might exist in those areas and then investigate specific clearance requirements. Security clearance is a status granted to individuals allowing them access to classified information (state or organizational secrets) or to restricted areas, after completion of a thorough background check. Then students download and examine the SF-86 form for security clearances (http://www.gsa.gov/portal/forms/download/116390) and create an instructional pamphlet for a student audience that includes tips on how to gain clearance and what to avoid that could prevent gaining security clearance. Students should examine the reasoning behind these security clearance requirements and include information in their pamphlet that demonstrates understanding of the rationale and its connection to the particular job and the function of the department. Sample issues may include the following: paying bills on time, drug and alcohol abuse, affiliations, and social media use.

3. Privacy, Liberty, Technology and the Constitution Debate

In order to further analyze Article 2 of the Constition and learn about specific surveillance programs and whether or not they are within the purvue of the president to execute, students begin by reviewing the Google Robot Defense video:
(http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-robot-defense-how-google-saw-privacy-before-snowden/)
or/and read the article: *Google argues for right to continue scanning Gmail* http://news.yahoo.com/google-argues-continue-scanning-gmail-083912032.html.

Students conduct further research if necessary in order to debate a position, in relation to Article 2 of the Constitution regarding whether these types of of surveillance programs are within the rights of the President not to get approval from Congress. The President, while having to enforce the law, also possesses wide discretion in deciding how and even when to enforce laws. The President also has a range of interpretive discretion in deciding the meaning of laws he must execute. In this case, the NSA 'Driftnet" programs have tested the bounds of presidential authority.

Finally, students culminate this work by making a recommendation to an executive decision maker on whether or not these programs are within the rights the President to execute/ how much discretion s/he should have in deciding the meanings of law executed. This prepares students to further debate, in unit seven, the ethical implications of such surveillance programs and whether they should exist at all.

4. U.S. Department Storyboard and Presentation on Cyber Security Issues

Students create a storyboard of the different departments within the Executive Branch of the Federal Government as they pertain to Cybersecurity (i.e. Department of Homeland

Security, Federal Trade Commission, National Security Agency, National Institute of Standards and Technology, Federal Bureau of Investigation, US Cyber Command). The storyboard should explain each department's role and their responsibilities Re: cybersecurity.

Then, in groups, the students compete to be the government department that best represents the federal entity that will develop universal cybersecurity standards for critical American infrastructure. Students choose from the following list: FBI (Federal Bureau of Investigation), NSA (National Security Agency), NIST (National Institute of Standards and Technology), DHS (Department of Homeland Security), and DOJ (Department of Justice).

Each group presents a PowerPoint that will advise the President of the United States on the topic of universal cybersecurity standards for critical American infrastructure. Each group presents their argument supporting why their group (department) should be selected to set universal cybersecurity standards.

Unit 3: Legislative Branch

In this unit, students examine the laws governing the online world, how they are created by the United States Congress (the Legislative branch), and how government is playing catch up as technology is developing faster than they can regulate. Students will first create a flowchart of the process of how a Bill becomes a Law, using the Patriot Act for example (a key law governing cyber security) as an example of this process. Students will then explore the differences between the functioning of the House and Senate in the filibuster for the Patriot Act in 2015 and create a Risk Assessment in regards to the expiring provisions of the Patriot Act. Finally, students will apply their knowledge of the legislative process to propose a new law that will help to regulate emerging technology that poses a potential cyber threat to government or citizens.

Unit 3: Key Assignments

1. How Do we Get that Law Again? - Flowchart

This assignment allows students to gain a general understanding of the US legal framework dealing with critical cybersecurity issues. Students research and create a flowchart which communicates how a bill becomes a law using the various bills that pertain to cybersecurity, such as the Patriot Act, as their subject matter. Students can post the flowchart as a blog or create it using presentation software like PowerPoint, Prezi, or Powtoon (http://www.powtoon.com). Students should demonstrate understanding of how a bill becomes a law as well as developing knowledge of the content of specific laws created by congress pertaining to cybersecurity.

2. Patriot Act Risk Assessment

After instruction in the differences between how the House and Senate function, students examine the fillibuster of the Patriot Act by Senator Rand Paul, (http://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469.html, http://www.usatoday.com/story/news/nation/2015/05/31/patriot-act-expires-senate-sta lemate/28260905/). Students then, based on existing knowledge, create a simple risk assessment, (like the one found here: http://www.ready.gov/risk-assessment) analyzing the potential risks and "blind spots" created by the controversial provisions of the Patriot Act that Senator Paul spoke out against.

3. Technology and Public Policy - Proposed New Law

Students now turn from focusing on laws specifically to analyzing emerging technology that may not have laws in place which would address cybersecurity threats that could emerge as a result of that new developing/new technology. Students research a new technological device or application that is just becoming popular. Though students have already researched bills and laws in assignments one and two, students may need to do additional research in existing laws or proposed laws that address emerging technology. Then, through discussion, students identify and analyze possible policies that could address the capabilities of the new information technology, such as, a new smartphone app that allows your texts to disappear so no one else can see them or "Snapchat" where one can send pictures that 'disappear' after a certain time period, which has been associated with human trafficking. Students can consider the following prompts in their preliminary analysis: 1) Should there be laws that govern the new technology? 2) Should there be age limits? 3) Parental controls? 4) Privacy? 5) Government supervision to thwart terrorism? Finally, in a communication medium of the teacher's choice, students propose a new law that should be applied to this technology, demonstrating understanding of the steps that would be required for it become a law.

Unit 4: Judicial Branch

A key role of the Supreme Court is reviewing the actions of the states, President and Congress and assuring their alignment to the Constitution with Judicial Review. In this unit, students analyze a key cyber privacy Supreme Court Case in Riley v. California and participate in a mock trial for this case. Students will then examine the Constitutional definition of treason and apply it to current events. Finally students will apply their knowledge of the court system and laws dealing with specific cyber threats in addressing a hypothetical cyber crime case.

Unit 4: Key Assignments

1. Judicial Review of Cyber Crime Laws, a Mock Trial

After an exploration of the role of the Supreme Court in Judicial Review, students are assigned a role in a mock trial (9 Supreme Court Justices with the rest of the class serving as lawyers for Riley or for the State of California). All students research Riley vs. California, a case in which the Court unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional. Then student lawyers, based on research, should prepare a written brief stating their legal cases according to which side they were assigned. Students then argue their briefs orally in front of the Supreme Court. Those students selected to be Supreme Court Justices will listen to, evaluate and question the oral arguments presented by both sides. After arguments, the justices will conference and then cast their votes. Supreme Court justices are responsible for writing and presenting their decision of the court.

Riley v. California: http://www.scotusblog.com/case-files/cases/riley-v-california/
Judicial Review: http://legal-dictionary.thefreedictionary.com/judicial+review

2. Treason Expository Essay

Students review Article 3 of the Constitution, which establishes the Supreme Court and the National Court System, and which seeks to define treason for the courts. According to Article 3, section 3 of the Constitution, "Treason against the United States shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort." Students review recent examples of treason that involve the disclosure of classified information (i.e. Bradley Manning). Identifying the attributes of classified information, students draw conclusions on classified information that requires protection of confidentiality, integrity, or availability and that should not be available to the general public. Students also watch the following two videos on security clearances to understand components of the process.
https://www.youtube.com/watch?v=j1cHEiZTRBM
https://www.youtube.com/watch?v=vLKFajcxzfY

Finally, students write an expository essay in which they analyze a new case study of treason. In that analysis, students should identify the ways the government and/or private companies could have better handled or conducted a security clearance in order to reduce the risk of someone disclosing information that could be exploited.

3. Legal Case Scenario Presentation

Students analyze a teacher defined imaginary case scenario of cyber-crimes or vandalism based on current events. The case should focus on one of the following areas: homeland security, public safety, privacy, freedom of speech, or intellectual property. Students then provide an analysis of the case scenario by specifying what laws or statutes it violates, what remedies could be provided, and what cyber security measures may be implemented to prevent future incidents. Students present the analysis formally in class. This assignment requires students to creatively apply legal knowledge dealing with specific cyber threats to critically analyze and resolve a problem.

Unit 5: The Election Process

A key component of the democratic process is the ability of citizens to choose their representatives, in others words to vote. Technology has created new avenues for political candidates to reach constituents and influence their voting behavior in a variety of ways. Students will begin by examining key voting issues, including those created by technology. Students will then look at the role of the Electoral College in selecting the President and analyze the feasibility of increasing voter turnout using online voting. Students will then examine the rise of political parties and make recommendations in a memorandum to a political candidate about how to use the internet in a way that protects the privacy of the electorate.

Unit 5: Key Assignments

1. Who Can Vote Timeline

Students work in pairs to create an online timeline (Capzles, Dipity, Meograph) that

depicts problems with voting security starting with the constitution to present day. Each timeline should include a minimum of 10 security issues throughout American history, and a minimum of 3-5 examples should identify electronic voting issues.
Research links: Problems with voting systems:
http://homepage.cs.uiowa.edu/~jones/voting/congress.html
http://www.cnn.com/2011/11/08/tech/web/online-voting/

2. Online Voting Feasibility Report

Students will examine the way in which the United States votes for President including the Electoral College, Election Day, the role of media, and how citizens vote at polls. Students will then explore the option to make voting more accessible for eligible voters by allowing online voting and will research online sources and their textbook to investigate and analyze the controversies surrounding online voting. Students will then draw conclusions on whether from a technical standpoint online voting can be made safe and secure, and if it would increase voter turnout. Since voting is regulated by the individual states, students will make a recommendation in the form of a written report to the governor of California making a case for either adopting or not adopting online voting for the reasons investigated.
http://www.cnn.com/2011/11/08/tech/web/online-voting/

Controversial Elections:
http://archive.fairvote.org/e_college/controversial.htm

Electoral Process
http://www.uen.org/themepark/liberty/electoralprocess.shtml

Digital Campaign
http://www.pbs.org/wgbh/pages/frontline/digital-campaign/

3. Ethics, Political Parties, and the Internet Memorandum

In this assignment, students begin by developing their knowledge of the U.S.'s track record concerning the manipulation and/or limitation of voting (from Alien and Sedition to voter registration laws to social media and electronic manipulation via voting machines) in order to make connections between these historical moments and the current political climate. Students research the rise of political parties and how those competing political groups have affected politicians' campaign strategies throughout history. Students also research how the gathering of data/information through social media and the like has changed the political debate and the nature of political races. Students then write an ethical use of the internet memorandum, identifying the ways in which the current mode of voter manipulation (see Narrowcasting doc for example) is a privacy issue and is connected to historical trends/moments. Students should also include ways to protect the privacy of the electorate in their memorandum. Students can utilize the following links to research and gain understanding:

Rise of Political Parties
http://philadelphiaencyclopedia.org/archive/political-parties-origins-1790s/

Internet and Politics
http://journalistsresource.org/studies/politics/citizen-action/research-internet-effects-po

litics-key-studies

The narrowcasting section
http://www.pbs.org/wgbh/pages/frontline/shows/persuaders/view/

1998 Politics and Internet
http://www.washingtonpost.com/wp-srv/politics/campaigns/keyraces98/stories/netizens101798.htm

Campaigning and the internet
http://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics/?_r=0

Unit 6: State Government

Each state in the Union has its own constitution and government system. These constitutions are the law of the land but are subordinate to the Federal Constitution. Here lies the political power struggle between the national and state government. Various states seek to carry out federal laws in different ways in both the real and virtual world. Students should begin their study through classroom instruction in this dynamic and the different powers that state and federal governments have as well as the mechanism through which states gain their individual power. Students then begin a data documentation project that allows them to track and categorize different cyberattacks, and in a fishbowl discuss various rules and laws on cyber security and privacy across different states and propose a new law that would address cyber attacks that are not covered by law. Next students will learn how this power struggle has lead to various disparate applications of federal law in different states through an examination of Health Insurance Portability and Accountability Act (HIPAA) requirements. Finally, students use this information to inform their community of their rights and protections under HIPAA.

Unit 6: Key Assignments

1. Tenth Amendment & Cyber Privacy Collage

After instruction in the Tenth Amendment and how federal and state laws interact, students use evidence, such as preliminary knowledge of federal HIPAA law and both federal and state data privacy laws to construct an electronic collage (using Powtoon,www.Powtoon.com for example) that depicts the constitutional powers of the state and federal governments. Based on this understanding, students develop a written conclusion on which government's powers supersede the other as it relates to cybersecurity that they add to their collage.

2. Letter of proposed legislation

Part One: Students begin this assignment by starting a data collection project. Students research and document findings Re: new cyber security breaches/exploits in a class or individual Cyber Laws Spreadsheet or database generated on Excel (or similar) application in order to track new exploits and hacking methods in order to stay current so their ongoing work will be informed by the most up to date information. Students will track the exploit/hack, cite the source that reported the hack, and identify laws that exist that address the issue and whether it is a state or federal law, or document that no law exists.

Part Two: Using information provided by the National Conference of State Legislators on state laws regarding cybersecurity (http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx) students engage in a class fishbowl discussion in order to discuss the differences and similarities that exist between California state data privacy laws, other state laws, and United States federal fata privacy laws. Then, students brainstorm potential new cyber security laws at both state and federal levels, considering the cyberhacks they documented in part one that had to no law that could address that issue. Finally, after identifying their state representative, students will write a letter to their state representative proposing a new law to support online privacy or cyber security, based on their understanding of existing California state law. In the letter of proposal, students will introduce themselves and describe the context of the research project, include a summary of current exploits documented in the research with proper citations of sources, an explanation of the proposed law and a rationale for the proposal. This proposed law should be informed by data documented in part one so students can address new network exploits that were not necessarily covered in previous or existing laws.

3. HIPAA and CA Research Paper

Students continue their investigation of state laws by reviewing provisions of the current US Health Insurance Portability and Accountability Act (HIPAA), and researching how it has been implemented in the state of California by the agencies responsible for implementation. Then students identify similarities and differences between HIPAA law with other similar state privacy laws that deal with storing individual’s information online. Students will write a research paper on their findings. Some of the criteria for comparison includes: (1) time requirement to report any hack activity (2) how citizens data is protected in each of the compared states (3) when citizens are informed after data breach that affects their personal records (4) levels of reporting with the state bureaucracy ie (report to one state agency or multiple agencies) and (5) available state agency/ies to help victims of data exploits and hacks. From this comparison students will draw conclusions from the research about what different states determine to be important about protecting individual’s information and will identify ways California specifically could improve the state’s practice and ways California could be a model for implementation of such laws. (Resource: http://www.ehcca.com/presentations/HIPAAWest1/stanton.pdf)

4. State v. Federal Cyber Security Blog

Working in teams, students evaluate, monitor, and ensure compliance with privacy rights violations in their state during past year. In order to identify whether or not the government has an obligation to inform citizens when there are cyber hacks that involves citizens’ private data, students investigate cases when government has failed to inform citizens of cyber hacks. In a blog, students classify each violation by providing an explanation of whether or not this has resulted in a violation of the Bill of Rights. This should be an open forum for students and the community to identify and discuss hacks within the government (state or federal) that were not reported, and to discuss how well the government protects individual civil rights and what private citizens should do to

protect themselves in order to make more informed choices through awareness of cyber laws and cyber exploits. Students will continue to research and update the blog once it is developed with news on the latest exploits, by recording the responsible party/ organization, the method of attack an analysis of whether civil rights were violated through a lack of reporting by the government.
https://oag.ca.gov/ecrime/databreach/list

Unit 7: Civil responsibilities v. Government responsibilities

Building upon knowledge of civil liberty and civil rights, this unit introduces current legal requirements and ethical standards, rights and restrictions governing technology, information systems, and digital media. Students read chapters on civil liberty and civil rights as introduced in textbooks such as *Magruder's American Government,* and chapters on legal and ethical issues as introduced in textbooks such as *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology,* before proceeding to assignments and course activities. Drawing on knowledge gained from their readings, students engage in several policy debates supported by critical arguments and evidence to acquire a deeper understanding of the tension between civil rights, government policy and technology. Finally, working in groups, students present their findings of research on their state's' compliance to privacy regulations.

Unit 7: Key Assignments

1. Discussion Board on Privacy, Liberty, Technology and the Constitution

Building on the work of assignment three in unit two and to prepare for the essay in the next assignments students review the Google Robot Defense video(http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-robot-defense-how-google-saw-privacy-before-snowden/) and read http://news.yahoo.com/google-argues-continue-scanning-gmail-083912032.html. Students then generate debate questions for an online debate using a discussion board that will allow them to discuss and analyze the ethical implications of government surveillance and how necessary it is for our security. This should prepare students to assess policy needs and collaborate to develop policies to govern information technology activities.

2. Analytical Essay on Government Surveillance of Citizens

Building on the work of the prior assignment, students watch the video "Spying on the Homefront" (http://www.pbs.org/wgbh/pages/frontline/homefront/), a documentary that explores the ethical issues surrounding the "driftnet" method, which allows the government to have access to citizen data in order to thwart a terrorist attack. After watching the documentary and conducting any additional necessary research Re; government's access to citizen data, students write an essay in which they analyze the government's actions as they pertain to protecting or violating citizens' constitutional rights and discuss their implications to democracy and society. Students are required to describe the ethical dilemma presented (access to citizen data by the government during wartime/conflict for the protection of citizens), identify the conflicting values, critically analyze the implications, and provide recommendations for government action. Students should use as evidence any and all information gathered information from the previous assignment that is relevant, as well as from prior units. This assignment will challenge students' analytical, critical thinking, and problem solving skills in facing ethical dilemmas.

Reference: Driftnet article, *Campaign To Justify Spying Intensifies* (http://www.washingtonpost.com/wp-dyn/content/article/2006/01/23/AR2006012300754.html).

3. Manual of Cyber Security Laws

Students reflect on assigned readings (chapters on legal and ethical issues as introduced in textbooks, such as *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*), and the work of prior assignments, and create a web gateway manual for navigating cyber security laws that identifies the key cybersecurity issues, including homeland security, public safety, privacy, intellectual property, and freedom of speech, and corresponding laws of the Constitution, Bill of Rights, and federal and state laws that govern given cybersecurity issues. The manual should list key cybersecurity issues, provide a weblink to their related laws and regulations through searching the Internet, and a single sentence description of the laws and regulations. The assignment enables students to demonstrate a general understanding of the US legal framework dealing with critical cybersecurity issues and synthesize and present in a concise manner information gathered in previous assignments for a new audience and purpose.

4. Community Outreach Poster

Building upon knowledge of US laws and regulations governing cybersecurity issues, students select one cybersecurity area of their interest (e.g., intellectual property protection) and conduct an in-depth research on the potential threats and related laws, regulations, as well as moral principles addressing the threats. Students then analyze government's roles and citizen's obligations and responsibilities in addressing the issue. Student develop a poster for public places, such as libraries, parks, or community centers, communicating their research and analysis as part of a community outreach event in order to educate the public about cybersecurity. The assignment is expected to develop student's awareness of civil responsibility in cybersecurity issues.

Unit 8: Evolution of Democracy

Integrating knowledge introduced in previous units, this unit explores topics such as how the virtual world is changing the role of Government, do the ideas of democracy still apply, and how we can formulate policies to meet the challenges. Students are required to conduct research on emerging technologies and their potential threats to civil liberty and democracy, engage in policy debate, and, working in groups, develop new policies and actions in addressing emerging cybersecurity threats.

Unit 8: Key Assignments

1. Emerging Cyberthreats Presentation

This assignment is intended to enhance student's understanding of the interaction and dynamics between American democracy and technology and aid them in answering the question, "do the ideas of democracy still apply in this new 'world.'" Students investigate emerging cyber threats to civil liberty and democracy by visiting websites, such as www.ted.com, www.blackhat.com, www.cert.org, www.us-cert.gov, etc. Students present the research in class and engage fellow students in class discussion seeking possible remedies to cyber place problems in order to protect civil liberty and democracy. Utilizing Google platforms, students present the emerging cyberthreats presentation. Students are expected to demonstrate capability to identify the trends of technological change and their impact on American government and democracy.

2. Argumentative Essay of Security Personnel

Using information and ideas gathered from unit 4 and unit 7, students write a narrative essay using Powtoon (www.powtoon.com) that includes a brief opinion of whether or not Edward Snowden, as a security clearance personnel, should have released classified information as an act of civil responsibility as a U.S. citizen. Students should include a written analysis of whether Edward Snowden's actions were of a patriot or a traitor. Students can do individual research or reference the links below, or a combination of both.

Reference: *Snowden on Cyber Warfare: We Really Started This Trend*
http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/snowden-on-cyber-warfare-we-really-started-this-trend/

Wired Article Edward Snowden:The Untold Story
http://www.wired.com/2014/08/edward-snowden/

3. Policy Arguments and Formulation on Preemptive Actions

Part I Policy Arguments

Students watch the Frontline video "United States of Secrets (part two)" (http://www.pbs.org/wgbh/pages/frontline/united-states-of-secrets/#united-states-of-secrets-(part-two), and develop at least two positions that would justify or disagree with the U.S. Government's preemptive policies and actions that have taken place over the last 2-years as described in the video.

Student may center on debating the following two policy issues:

1) Whether or not the US should have a centralized national ID system operated by the federal government amid the concerns of homeland security, public safety, illegal immigrants, identify theft concerns, challenging the foundations of US democracy.
2) Whether or not the US should eavesdrop or launch government assisted cyber attacks to foreign governments in the mid of homeland security concerns.

Students present their policy arguments in a class discussion.

Part II Policy Formulation

Working in groups, students partner with a classmate that has the opposite viewpoint on their policy issue and develop a policy paper that would satisfy national security as well as civil liberty. In the policy paper, students specify what actions the government should take to address the concerns raised through their issue, provide justifications with evidence for the actions, and identify and discuss implications to democracy as a result of the action.

Course Materials:

Textbooks:
District adopted Government

Title: *Magruder's American Government*
Author(s): McClenaghan
Year published: 2004
Publisher: Pearson Prentice Hall
Student edition text: ISBN 0131816764

Cybersecurity

Basse, Sara. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*. 4th ed. Upper Saddle River, NJ: Pearson Education, Inc.

National Initiative for Cybersecurity Education
https://www.fbcinc.com/e/NICE/default.aspx