United States Cybersecurity Council

Background Guides

Committee Topics:

1. *Consumer Data Privacy*
2. *Ransomware and Infrastructure Cybersecurity*

Stanford Model United Nations Conference XXV

Committee Chair – Jay Yu, Class of 2025

Table of Contents

Topic 1: Consumer Data Privacy

Letter from the Chair 4

Background and History 6

European Union: General Data Protection Regulation (GDPR), 2016 6

Principles *6*
Scope and Aims *7*
Enforcement and Effect *8*

China: Personal Information Protection Law (PIPL), 2021 12

Scope and Aims *12*
Enforcement and Effect *14*

California: California Consumer Privacy Act (CCPA), 2018 16

Scope and Aims *17*
Enforcement and Effect *18*

Current Situation 20

Questions to Consider and Committee Tasks 22

Task 43

Points of Consideration 43

Additional Sources and Reading 23

General Background 23

GDPR 23

PIPL 23

CCPA 23

Works Cited 25

Table of Contents

Topic 2: Ransomware and Infrastructure Cybersecurity

Letter from the Chair 4
Background and History 28
Overview of Ransomware 28
First Ransomware Attacks 29
Reveton, 2012 – Cryptocurrencies and Ransomware-as-a-Service 29
WannaCry, 2017 – Global Institutional Targets with State-backed Actors 31
DarkSide, 2021 – The Colonial Pipeline Attack and the “Honorable Thief” 35
The Future of Ransomware — Ransomcloud and the IoT 37
Current Situation 40
Modern Ransomware Traits 40
Federal Enforcement and Legislation 40
Questions to Consider and Committee Tasks 43
Task 43
Points of Consideration 43
Additional Sources and Reading 44
Ransomware History and White Papers 44
Case Studies 44
Ransomware Legislation Recommendations 45
Works Cited 46

Topic 1:
Consumer Data Privacy

Measures to Prevent Misuse and Exploitation of Private Consumer Data

*Developing a comprehensive **Consumer Data Privacy Act***

United States Cybersecurity Council

Stanford Model United Nations Conference XXV

Letter from the Chair

Esteemed delegates and honorable guests,

I am Jay Yu, Class of 2025, currently pursuing a double major in Computer Science and Philosophy & Literature. On behalf of the Model UN team and the Society for International Affairs (SIAS) here at Stanford, welcome to SMUNC 2022! It is my honor to serve as your chair for the United States Cybersecurity Council.

Cybersecurity is a topic incredibly important to me both academically and personally. Growing up in Shanghai, China, I have witnessed first-hand the trade-offs that widespread technological disruption inevitably brings: increased conveniences for decreased privacy; economies-of-scale for vulnerabilities of scale; enhanced administrative efficiency for enhanced surveillance potential. It is these personal experiences that have persuaded me to pursue my dual academic journey in Computer Science and Philosophy here in the heart of Silicon Valley, trying to understand what entrepreneurs' catchphrases mean for the real world, and figuring out where the technology ends and where the policy begins.

The United States Cybersecurity Council is a specialized committee for SMUNC 2022, set up to simulate a joint meeting between US government officials and industry leaders to brainstorm cybersecurity legislation, ultimately producing documents formatted as traditional Model UN resolutions, to be passed or rejected by the entire council. Because of the multi-faceted nature of cybersecurity, this council will have two different debate topics. The first topic considers cybersecurity from a personal, consumer level: the question of consumer data privacy. The second topic approaches cybersecurity from an industrial, institutional perspective: the question of how to fortify critical industries and national infrastructure against ransomware cyberattacks. Delegates are invited to prepare for both topics, and we will vote during committee the order of debate. Depending on the status of debate, the chair may also introduce one or two crisis elements for each debate topic.

In addition to having "regular" delegates in the committee, this committee will also have a few "chameleon delegates" that take on different roles for each topic, in order to have more topic-specific viewpoints and increase relevance of diverse parties for each topic. An example is the "Consumer Financial Protection Bureau / Bank of America Representative." The CFPB is extremely relevant to the topic of data privacy, but not so much to the topic of infrastructure defense. On the other hand, the banking industry is a critical part of national infrastructure (even though it is privatized) that it needs to be considered when developing a comprehensive

infrastructure cyber-defense act. “Chameleon delegates” are given as a challenge to experienced delegates and are encouraged to prepare two position papers outlining their roles for each topic.

I firmly believe that understanding the powers and limitations of modern technology is a key step to understanding the challenges of our modern world. As members of the US Cybersecurity Council, I hope you can join me on this journey to understand the social, political, and ethical ramifications of our powerful modern technologies, producing effective resolutions and fruitful debate.

Sincerely,



Jay Yu
United States Cybersecurity Council Committee Chair
SMUNC 2022

Background and History

In an era where technology permeates every facet of our lives, the protection of individual data privacy has become a question of incredible importance. An overwhelming number of Americans have expressed concerns over how their personal data is being handled: approximately 70% of Americans believe that their personal data is less secure than five years ago, 79% believe that private companies are tracking too much consumer data, and 64% believe that the government is tracking too much consumer data (Auxier).

With continuous reports of data mishandling by tech giants, governments around the world have begun to place a strong emphasis on personal data privacy over the last decade. The following section of this background guide will dive in-depth into three particular data privacy policy examples, implemented by the European Union, the People's Republic of China, and the state of California. Through comparing and contrasting the main tenets of these three pieces of legislation, this piece hopes to convey the design choices, tradeoffs, and implications in formulating a comprehensive consumer data privacy law for the United States at the federal level.

European Union: General Data Protection Regulation (GDPR), 2016

Principles

The European Union's General Data Protection Regulation (GDPR), adopted in 2016 and enforceable beginning 2018, is perhaps one of the earliest and most well-known comprehensive

data protection regulations in the world. The overarching principles of the GDPR are as follows (GDPR, Articles 5.1-2):

1. **Lawfulness and transparency**, processing must including documentation of purposes
2. **Purpose limitation**, data may only be processed for documented purposes
3. **Data minimization**, not collect more data than strictly necessary
4. **Accuracy** of personal data collected
5. **Storage limitation**, must dispose of data after done with specified purpose
6. **Integrity and confidentiality**, processing must be done to ensure personal privacy, through using encryption and other means
7. **Accountability**, the institution conducting data processing must demonstrate ability and will to comply with GDPR

Scope and Aims

The scope of the GDPR is incredibly broad. Any company in the world that processes the data of EU citizens or offers online services to EU citizens is applicable to the GDPR ("What is GDPR"). This means that multinational tech companies such as Google, Facebook, and Amazon that offer services in Europe must comply with the GDPR. The broad reach of the legislation has pushed tech companies around the world to maintain higher data privacy standards and has also encouraged governments around the world to impose similar data privacy legislations.

The scope of "personal data" is also interpreted broadly. It is defined to include all "information related to an identifiable natural person… directly, or indirectly" (GDPR, Article 4.1). This

definition thus includes modern online identifiers such as IP addresses, location data, cookies, online autofills, and other "indirect identifiers" which previous legislation often overlooks.

Under the GDPR, personal data may only be "processed" — defined to include modification, storage, retrieval and deletion (Article 4.2) — under one of six conditions (Article 6):

1. **Unambiguous consent** from the data subject (the "user")
2. **Contractual obligations** and preparations, eg. Background checks
3. **Legal obligation** to comply with court orders
4. **To save someone's life**
5. **Public interest** or official function tasks
6. **Legitimate interest** to process someone else's data

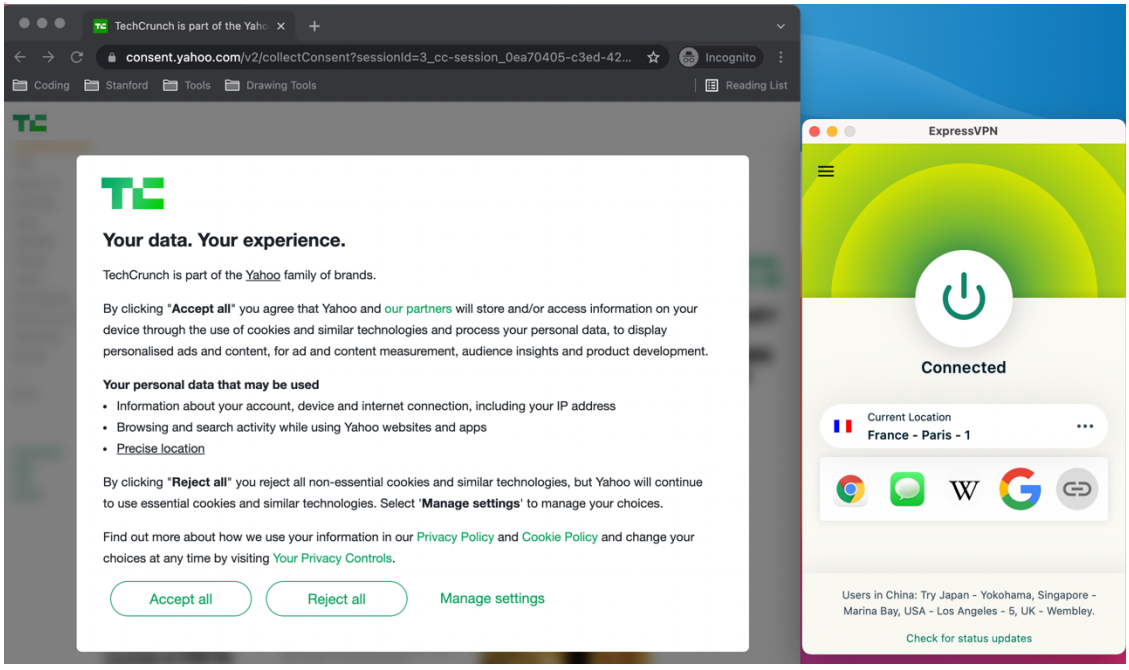
The sixth condition is a flexible and "catch-all" clause widely open to interpretation. Companies need to individually identify and define what this "legitimate interest" may be, and provide documentation of said interest ("Legitimate Interest"). In all cases, the GDPR requires companies to document the basis for information processing and notify the subjects ("What is GDPR"). However, the GDPR does not specify a standard there is no standard for what this "documenting" may entail. Thus, companies are given significant latitude in their implementation of the GDPR: they are able to **self-identify "legitimate interests"**, **self-style "consent banners,"** and **self-format "privacy documentation."** This question of company discretion and flexibility is an important issue to consider when crafting a comprehensive data privacy legislation.

Enforcement and Effect

The main method of enforcement is through fines, which may be up to 4% of a company's annual revenue. Considering that Amazon's annual revenue for 2020 was $386 billion (Statista), which is $60 billion more than the same-year GDP of Denmark (World Economics), the upper limit of a GDPR fine could be enormous. As some commentators humorously note, "What do Google, British Airways, H&M and Marriott all have in common? Well, they all received fines in excess of €10,000,000 for GDPR violations relating to personal data" ("GDPR Fines and Penalties"). In addition to this administrative fine, individual users also have a right to compensation if the misuse of data has had a negative material or non-material impact on their lives.

Effects of the GDPR are also visible when browsing different sites. As shown in the figures below, when notable American tech media outlet TechCrunch is visited with a European IP address, the user will be directed to a GDPR consent banner, where the user has the option to

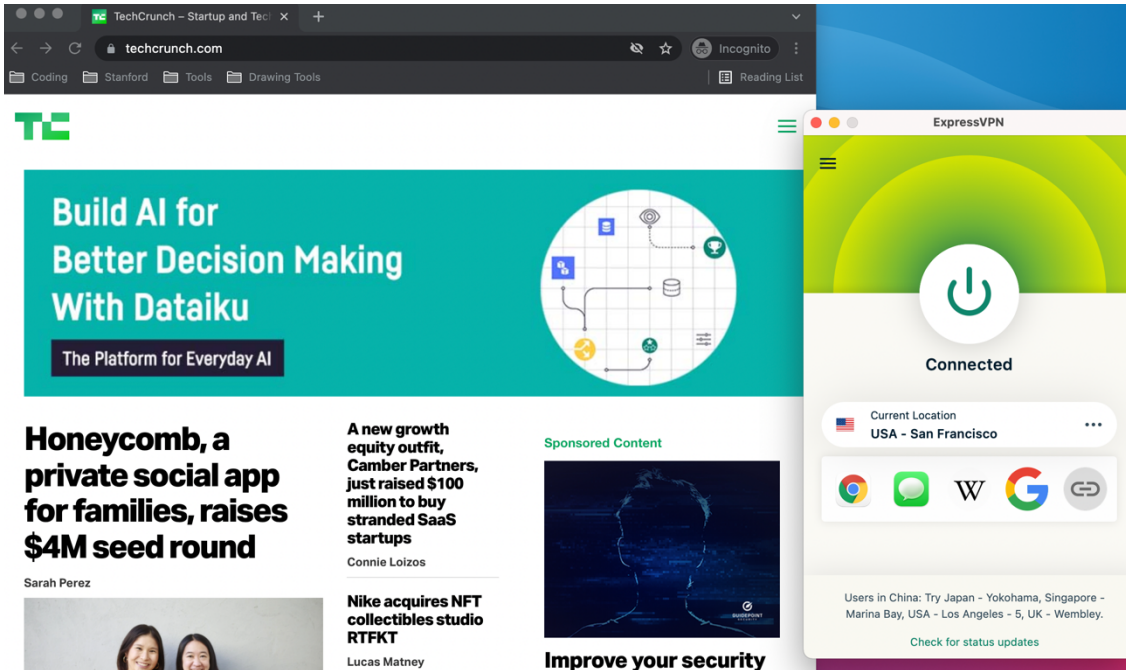
Figure 1: TechCrunch website accessed via European IP address



accept or reject the website's use of personal data before being directed to the content of the website. If the user clicks on "Reject all," the functionality and articles on the website are still all accessible. On the other hand, this consent banner is not visible when approached using an American IP address. In this latter case, the website goes straight to its front page and will by default track users' personal data (device information, browsing activity, location as mentioned above), to be used in targeted advertising.

Though the implementation of GDPR arguably has achieved its intended aim on increasing cybersecurity standards, implementing a blanket data privacy regulation also has its economic costs. Most researchers agree that while the GDPR did indeed reduce online data sharing, it also decreased investment in EU technological startups relative to other markets, as well as increased costs for tech companies (Jia et al.). In addition, there was a marked drop-off in business for small online analytics and advertising companies, leading to an increased industry concentration for tech giants such as Google (Peukert et al.). Moreover, a new private industry of GDPR policy compliance was born — with many companies needing to adapt to the new regulatory rules, they would often hire external compliance consultants specifically for GDPR adaptations (Rand). This

Figure 2: TechCrunch website accessed via American IP address



post-GDPR research has exposed several tradeoffs of the policy and raises several questions. Does stopping companies from selling personal data significantly hurt the digital economy, and if so, should this data-selling be allowed? Should we allow a more concentrated analytics market, even if market players abide by higher regulatory standards? Should governments provide transitional subsidies to aid smaller companies in transitioning to GDPR rules or leave it to this new private market?

In addition to the aforementioned direct effects of the GDPR, the policy arguably has a greater impact in shifting the Overton window for data privacy legislation, being one of the first and most comprehensive of its kind. The wide scope of the GDPR has also forced multinational companies around the world to adopt these standards, as shown in the TechCrunch example. Furthermore, given the EU's international reputation for legislative rigor, many different countries have followed suit in pursuing similar data privacy laws, including South Korea's Personal Information and Privacy Act, Brazil's General Personal Data Protection Law, and Turkey's Data Protection Law. Thus, should the US also decide to establish a comprehensive data privacy act, legislators must consider the indirect impacts of such a legislation upon shifting the national and international conversation surrounding data privacy, setting the agenda and a positive example on how to protect individuals' inalienable rights regarding online data.

China: Personal Information Protection Law (PIPL), 2021

China's Personal Information Protection Law, which has just been passed in August 2021 and enforced starting November 1st 2021, is another exemplar of a comprehensive personal data

protection law. With many statutes and definitions inspired by the European GDPR, the PIPL provides a similar framework to protect personal information for Chinese citizens. However, within the PIPL there is a stronger emphasis on national security. With data sovereignty being an increasingly heated part of the debate over personal data laws, it may be useful to analyze Chinese legislative articles designed to enhance governmental control of cross-border data transfers.

Scope and Aims

The application scope of the PIPL is very broad, similar to the GDPR. The law applies to all companies operating in China, as well as foreign companies processing, analyzing, or providing services to Chinese citizens (Article 3). Furthermore, the PIPL adopts a similar definition of "protected data" to the GDPR, suggesting that all "all kinds of information… related to identified or identifiable person" is under its purview.

Data may only be processed under the PIPL under the following circumstances (Article 13):

1. **Obtaining individuals' consent**
2. **Contractual obligations** and preparations
3. To fulfil **legal responsibilities**
4. To respond to **public health incidents or protect citizens' lives** or livelihoods under emergency conditions
5. Handling personal information for **news reporting**, public opinion supervision, or other activities in the public interest

6. Handling personal information **already disclosed** under other legal frameworks
7. **Other circumstances** provided in laws and administrative regulations

As shown, many of the data processing circumstances within the PIPL are similar to the GDPR, particularly 1-4. The most notable difference is the replacement of a "legitimate interest" clause in the GDPR with a generic "other circumstances" clause. While both clauses are flexible and open to interpretation, the GDPR's "legitimate interest" clause provides companies with an interpretive back door, whereas the PIPL's "other circumstances" provide the government and enforcement agencies with more leeway and thus broader authority.

Interestingly, the PIPL also has an entire section of special articles relating to the data processing by government agencies. Articles 33-37 explicitly state that governmental agencies are also liable to storing private citizens' data according to the aforementioned standards in Article 13. In addition, government agencies must also not store more data than is strictly necessary and may not transfer data abroad without prior approval.

As mentioned before, the PIPL has a very strong national security undertone, containing a variety of national security clauses. This includes strict regulations on the preconditions for international data transfers. All international commercial data transfers must satisfy one of the following pre-conditions (Article 38):

1. Pass a security assessment by the state cybersecurity enforcement agencies
2. Undergo special personal information protection sanctioned by the state

3. Have a contract with a foreign data receiver sanctioned by the state
4. Other conditions according to state cybersecurity guidelines

If citizens' data are transferred abroad, Article 39 also states that related individuals need to be notified of the foreign recipient, handling purpose, and contact information. This strict localization of data allows the Chinese government to use citizens' data as a political tool. The concept of "data sanctions" is implicitly acknowledged in Article 43, suggesting that any country adopting discriminatory data withholding practices against China may be subject to "reciprocal measures."

Other notable additions that the PIPL contributes to the debate over data privacy policy includes the concept of a "data inheritance," in which individually exercisable data privacy rights of a deceased individual are automatically transferred to the next-of-kin (Article 49).

Enforcement and Effect

Punishments for violating the PIPL are extremely severe. A company may be fined up to 5% of its annual revenue (Article 66), and may also face suspension of services in China. "Directly responsible individuals" may also be personally fined, and temporarily banned from serving in any leadership position within the company (Komnenic). Though it is too early to tell how these enforcement measures are wielded in practice, in theory the PIPL provides a much harsher punishment to violators than the GDPR. Making company leaders personally liable for certain punishments may also prove to be a more effective deterrent than simply fining the company.

The concept of "platform self-regulation" is a particularly interesting part of the PIPL. Article 57 suggests that online platforms, such as App Stores, cloud services, and other media platforms have an obligation to self-regulate according to three principles:

1. Have an independent board of outside supervisors monitoring personal data handling
2. Stop providing services to products/services that violate PIPL or other laws
3. Regularly release public reports detailing personal information protection status

This article is primarily targeted at China's tech giants such as Alibaba, Tencent, Baidu, and ByteDance, and represents a novel approach also known as a "gatekeeper" policy, where large companies are allowed to self-implement these policies (Lee et al.), akin to Facebook's Oversight Board. This approach could be fruitful in a US comprehensive data privacy policy, as it allows for sufficient autonomy for large companies to tailor their own implementation approach. If companies do not adhere to these policies, it could also provide a stronger legal basis for regulatory authorities to challenge these companies' practices in court.

Perhaps one of the challenges for China implementing PIPL is the question of whether the government can regulate itself. Within PIPL, Article 68 stipulates that government offices violating PIPL shall be held responsible by their superior offices, a much vaguer, and arguably lighter punishment than those specified for private companies. Whether or not this mechanism is effective in preventing government misuse of personal data is still unclear. Nonetheless, PIPL represents an important step in China recognizing the government's own responsibilities in

protecting citizens' data, and the special emphasis on government data-handling cases is something that many other data privacy laws, including the GDPR, generally tend to overlook.

Lastly, the PIPL's emphasis on national security may also be a global signal on the debate of data sovereignty. Though China has always been known to prioritize national security concerns over free information flows, the implicit authorization of "data sanctions" and strong emphasis on localized storage of user data represents a new level of citizens' data being weaponized as a political and diplomatic tool. Whether or not other countries will also follow suit in this fashion of "data nationalism" is still unclear, but these actions should prompt US policymakers to consider how much of citizens' information should be allowed to flow across borders to foreign servers. For multinational tech companies, it also poses a question of whether or not they should regionalize and compartmentalize operations to certain geographic spheres to abide by different sets of regional regulations, thus possibly creating a "splinternet" effect.

California: California Consumer Privacy Act (CCPA), 2018

Though the US does not have a comprehensive national data privacy law, some states have implemented their own data protection policies. The most notable and comprehensive of these is California's Consumer Privacy Act (CCPA), passed in 2018 and put into effect on Jan 1st 2020. The CCPA is a significant landmark in US data privacy policy, as it is likely that other states will follow suit with similar data privacy laws and could pre-empt a federal data privacy law (Mulligan et al., 38).

Scope and Aims

The scope of the CCPA is somewhat narrower than the GDPR and the PIPL, though still considerably broad. Companies subject to the CCPA *must be for-profit*, collects information of Californians, and is subject to one of the following threshold criteria (CCPA, Article 1798.140)

1. Have a gross annual revenue of over $25 million USD
2. Buy, sell, receive personal information of over 50,000 California residents, households, devices
3. Derive 50% of annual revenue from selling California residents' personal information.

Thus, the CCPA excludes targets such as government agencies and other non-profit institutions, which are applicable targets of other privacy laws such as the PIPL. The definition of information in the CCPA is also similar to the GDPR and the PIPL, defining to be "any information that identifies, relates to, or could be reasonably linked to you or your household," that is not already publicly available in government records ("CCPA FAQ").

Unlike the GDPR and PIPL, the CCPA uses an "opt-out" framework instead of an "opt-in" framework ("CCPA vs. GDPR"). This means that the CCPA does not have any "bases for processing" for businesses, as these "bases" are built for an opt-in framework. Instead, the CCPA focuses on enumerating "data rights" that California residents have over their data (Mulligan et al., 38):

1. Right to know, be aware of what data is being collected
2. Right to opt-out, or decline a business from processing the individuals' data

3. Right to delete, or delete any current data that the business has of the individual

Enforcement and Effect

Unlike the GDPR and the PIPL, the CCPA does not fine companies according to a certain percentage of annual income. Instead, it fines per violation: up to $2500 for an unintended violation and $7500 for an intentional violation. These violations can add up very quickly — just 10,000 pieces of data not adhering to the standards may be fined $25 million, and the CCPA does not set a limit on the maximum total fines possible.

Arguably, the CCPA's focus on an opt-out framework can sidestep many of the economic downsides that the GDPR has brought, thus minimizing the impact of the legislation on business operations. However, this opt-out framework may also defeat the original purpose of the legislation. Without a standardized way to opt-out of a personal information being tracked, companies can make it very difficult for consumers to opt-out of their information being tracked.

Recall the example of TechCrunch shown in Figures 1 and 2. Theoretically, when accessed from an IP address from San Francisco, the TechCrunch site should be compliant with CCPA standards. Yet, it is unobvious where on the site a user could stop the website from tracking personal information — something that the GDPR-protected version of the site had no problem with. Suppose that the average user does not have any background in data privacy. Under the GDPR, the user accessing the TechCrunch website would be directly informed and could actively choose whether to have cookies tracked. The user would walk away aware that the

website asked for their consent. On the other hand, under the opt-out design of the CCPA, the user could browse the entire site and be oblivious to the fact the website was tracking them. The opt-out model of the CCPA thus raises the question: is a lack of negative consent equal to free permission to distribute consumers' data?

Current Situation

There is no single comprehensive, national, and effective data privacy law in the United States (Mulligan et al., 1). Though there are some state-level comprehensive data protection laws, such as the CCPA introduced in the previous section, all federal laws related to consumer data privacy are narrow, sectoral, and enforced by multiple agencies.

This maze of legislation has meant that oftentimes there is "overlapping and contradictory protections" (O'Conner), as well as a loss of consumer confidence in data protection. Furthermore, most of the laws described above were enacted decades ago, built for technology used in another era. With the advent of modern technologies such as the Internet, these legislative acts have become greatly antiquated.

The table below loosely summarizes this current patchwork of policies:

Figure 3: Overview of Federal Data Privacy Legislation

Legislation	**Target**	**Jurisdiction**	**Reference**
Federal Trade Commission Act (FTC Act), 1938	Targets "Unlawful or deceptive acts or practices" (UDAP) "in or affecting commerce", applicable to deceptive data tracking practices. Often cited in data privacy cases, but powerless over banks, insurance companies, carriers and internet service providers.	Federal Trade Commission (FTC)	Mulligan et al., 30
Fair Credit Reporting Act, 1970	Consumer's creditworthiness may only be used for "certain permissible purposes," but no measures explicitly stating individuals' consent is necessary to store such data	FTC, Consumer Financial Protection Bureau (CFPB)	Mulligan et al., 12

Family Educational Rights and Privacy Act (FERPA), 1974	"Materials which contain information directly related to a student" that is maintained by an "educational agency or institution." Student may request to view data, control disclosure, challenge inaccuracies.	Department of Education	Mulligan et al., 20
Health Insurance Portability and Accountability Act (HIPAA), 1996	Targets individually identifiable "protected health information" held by healthcare providers, health plans, clearinghouses, and associated entities.	Department of Health and Human Services (HHS)	Mulligan et al., 11
Children's Online Privacy Protection Act (COPPA), 1998	Prohibits websites and online services from collecting "personal information" from children below 13 without "verifiable" parental consent. Must have a "prominent and clearly labelled link" to an online notice of privacy policies on its home page.	FTC, State Attorney Generals	Mulligan et al., 21
Gramm-Leach-Bliley Act (GLB), 1999	Targets "Consumer non-public information" held by financial institutions. Requires consumer consent to share data with third parties.	CFPB, FTC, Federal banking authorities	Mulligan et al., 9

As shown, the most common enforcement agency in data privacy cases is the FTC, the self-described "top cop on the privacy beat" (Pahl), using primarily the statue within the FTC Act giving the agency permission to prosecute cases of "unlawful or deceptive acts and practices." However, this vague clause can only go so far in pursuing higher standards of data privacy. The law does not mandate any form of user consent and is very restrictive in scope — far more so than the three comprehensive data privacy laws outlined above.

Moreover, as the rapid increase of publicized cybersecurity disasters in recent years has highlighted that a piecemeal strategy for data privacy is untenable in the long run (O'Conner).

Thus, there needs to be a paradigm shift in data privacy protection: a holistic, well-crafted, and up-to-date legislative framework that makes responsibilities clear for consumers, businesses, and the federal government.

Questions to Consider and Committee Tasks

Task

The overarching committee issue is stated as: *Measures to Prevent Misuse and Exploitation of Private Consumer Data Developing a comprehensive* ***Consumer Data Privacy Act***. This Consumer Data Privacy Act is implemented at the federal level. By the end of debate time, the committee should have a draft resolution formatted in MUN-style, with preamble and operative clauses.

Points of Consideration

The following are points of consideration to aid with developing a comprehensive resolution. This is by no means an exhaustive list of all the points you may want to consider.

1. Should this Act be on an opt-in (like GDPR and PIPL) or opt-out (like CCPA)? If the former, what are to be the "bases of processing"? If the latter, how easy and visible should the opt-out option be?
2. What is to be the scope of application of this law? For-profit companies, government agencies, or all organizations? Are there any specific thresholds, such as those defined in the CCPA?
3. Should this law also have provisions discussing concepts related to national security, such as data localization, data sovereignty, and limitations on foreign transfers?

4. What are the legal punishments for violators? How are fines determined? Should there be broader punishments, such as suspension of operation?
5. Which agencies will enforce this new law? The FTC or perhaps a newly created agency? How does this new law interact with both legacy laws and state laws such as the CCPA?
6. How can the average American citizen benefit from this law in everyday life?

Additional Sources and Reading

General Background

2019 Congressional Report on Data Protection Law (Mulligan et al.):
https://crsreports.congress.gov/product/pdf/R/R45631

2017 FTC Blog Post on Data Privacy:
https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat

2012 FTC Privacy Report:
https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

GDPR

What is GDPR, explained: https://gdpr.eu/what-is-gdpr/

GDPR Full Text:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2021 Academic Paper Detailing Economic Impacts of GDPR:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560392

PIPL

PIPL Full Text, Chinese:
http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

PIPL Full Text, Translated by Stanford DigiChina:
https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Stanford DigiChina Analysis of PIPL:
https://digichina.stanford.edu/work/chinas-draft-privacy-law-adds-platform-self-governance-solidifies-cacs-role/

Deloitte Analysis of PIPL:
https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html

CCPA

California Attorney General Brief of CCPA: https://www.oag.ca.gov/privacy/ccpa

CCPA Full Text:
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

CCPA vs. GDPR Comparison: https://www.gdpreu.org/ccpa-vs-gdpr/

Works Cited

"Annual net revenue of Amazon from 2006 to 2020." *Statista*, n.d. https://www.statista.com/statistics/266289/net-revenue-of-amazon-by-region/. Accessed 12 Dec 2021.

Auxier, Brooke. "Key takeaways on Americans' views about privacy, surveillance and data-sharing." *Pew Research Center*, 15 Nov 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/. Accessed 12 Dec 2021.

Bonta, Rob. "California Consumer Privacy Act (CCPA)." *State of California Department of Justice*, n.d. https://www.oag.ca.gov/privacy/ccpa. Accessed 14 Dec 2021.

Creemers, Rogier. "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021." *Stanford DigiChina*, 7 Sep 2021. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. Accessed 14 Dec 2021.

"Denmark GDP." *World Economics*, n.d. https://www.worldeconomics.com/GrossDomesticProduct/Denmark.gdp. Accessed 12 Dec 2021.

"GDPR Fines & Data Breach Penalties." *GDPR - User-Friendly Guide to General Data Protection Regulation*, n.d. https://www.gdpreu.org/compliance/fines-and-penalties/. Accessed 12 Dec 2021.

Jia, Jian. "The Short-Run Effects of GDPR on Technology Venture Investment." *Social Science Research Network*, 5 Mar 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912. Accessed 13 Dec 2021.

Komnenic, Masha. "PIPL: China's Personal Information Protection Law." *Termly*, 7 Dec 2021. https://termly.io/resources/articles/pipl/. Accessed 14 Dec 2021.

Lee, Alexa. "China's Draft Privacy Law Adds Platform Self-Governance, Solidifies CAC's Role." *Stanford DigiChina*, 3 May 2021. https://digichina.stanford.edu/work/chinas-draft-privacy-law-adds-platform-self-governance-solidifies-cacs-role/. Accessed 14 Dec 2021.

"Legitimate Interests." *UK Information Commissioner's Office*, n.d. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. Accessed 13 Dec 2021.

Mulligan, Stephen et al. "Data Protection Law: An Overview." *Congressional Research Service*, 25 Mar 2019. https://crsreports.congress.gov/product/pdf/R/R45631. Accessed 12 Dec 2021.

O'Connor, Nuala. "Reforming the U.S. Approach to Data Protection and Privacy." *Council on Foreign Relations*, 30 Jan 2018. https://www.cfr.org/report/reforming-us-approach-data-protection. Accessed 12 Dec 2021.

Pahl, Thomas. "Your cop on the privacy beat." *Federal Trade Commission*, 20 Apr 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat. Accessed 14 Dec 2021.

Peukert, Christian. "Regulatory Spillovers and Data Governance: Evidence from the GDPR." *Social Sciences Research Network*, 20 Apr 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560392. Accessed 13 Dec 2021.

"Protecting Consumer Privacy in an Era of Rapid Change." *Federal Trade Commission*, 30 Mar 2012. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Accessed 12 Dec 2021.

Rand, David. "The first unintended consequences of GDPR." *Hewlett Packard Enterprise*, 26 Feb 2019. https://www.hpe.com/us/en/insights/articles/the-first-unintended-consequences-of-gdpr-1902.html. Accessed 13 Dec 2021.

"The China Personal Information Protection Law (PIPL)." *Deloitte*, n.d. https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html. Accessed 13 Dec 2021.

"What is GDPR, the EU's new data protection law?." *GDPR.eu*, n.d. https://gdpr.eu/what-is-gdpr/. Accessed 12 Dec 2021.

"中华人民共和国个人信息保护法." 全国人民代表大会, 20 Aug 2021. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml. Accessed 14 Dec 2021.

Topic 2:
Ransomware & Infrastructure Cybersecurity

Measures to Prevent Malicious Ransomware Cyberattacks on Critical National Infrastructure and Industries

*Developing a comprehensive **Ransomware and Infrastructure Cybersecurity Act***

United States Cybersecurity Council

Stanford Model United Nations Conference XXV

Background and History

Overview of Ransomware

Ransomware is a type of computer malware that will infiltrate victims' computer systems, encrypt all files to make data inaccessible, then demand a ransom, often in hard-to-trace cryptocurrencies, in order to make the files accessible again ("Combatting Ransomware", 11). Combining the technical exploitation of system backdoors with the psychology of demanding a ransom for data held hostage, ransomware attacks have proliferated, from a relatively niche area of cybercrime to one of the "most dangerous threats facing enterprises," and they are highly disruptive to victims and lucrative to attackers ("Targeted Ransomware", 1).

In recent years, the barrier to entry for ransomware has also been significantly lowered, with the introduction of "Ransomware-as-a-service" (RaaS), where criminals can essentially purchase off-the-shelf ransomware kits to launch cyberattacks. As of 2020, researchers have found that RaaS attacks comprise of approximately two-thirds of all ransomware attacks ("Ransomware Uncovered", 7).

As highly publicized ransomware attacks of Colonial Pipeline, JBS Foods, and other critical industries, ransomware is not just an economic problem for targeted victims, but also a wider social problem. These attacks are often concentrated on public facilities such as hospitals, schools, police stations, and even city governments and US military facilities ("Combatting Ransomware", 3). As such, developing a robust legislative framework to counteract the threats of

ransomware and creating private-public partnerships on dealing with the issue are crucial to mitigating the socioeconomic risks associated with ransomware in a highly digitized world.

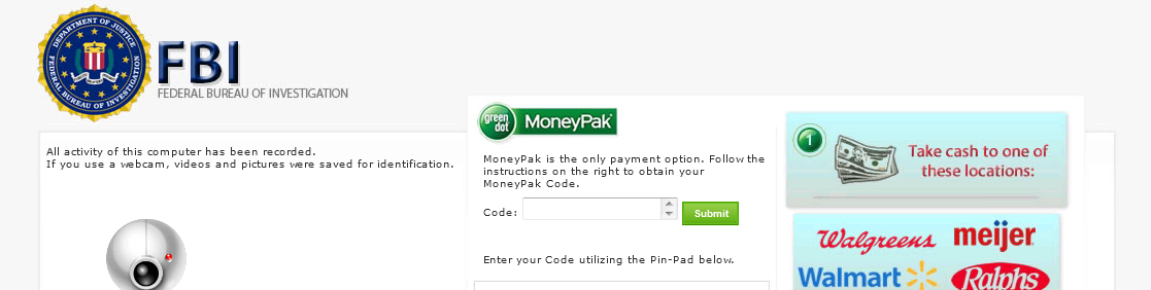
First Ransomware Attacks

Ransomware attacks have been around since the 1980s, with the first documented ransomware attack being a floppy-disk attack against AIDs researchers in 1989 (Harford). Joseph Popp, a Harvard-educated biologist, used a simple Trojan-horse attack mounted on floppy disks. Once the floppy disk was mounted onto the user's machine, it used a simple encryption algorithm to encrypt and lock all files on the users' disk and demanded a $189 ransom. Fortunately, since the encryption mechanism was very simple, users' files were quickly recovered by cryptography specialists.

Since then, ransomware gradually become more sophisticated and industrialized. In the early 2000s, as the Internet became accessible to ordinary households and emails were popularized, a new wave of ransomware was born, mass targeting households through phishing emails (Think: "Nigerian Prince" emails with malicious links) and demanding a small payment — around $20 each — for each (Harford).

Reveton, 2012 – Cryptocurrencies and Ransomware-as-a-Service

Ransomware really took off with the advent of cryptocurrencies such as BitCoin in 2009, which made ransom payments hard to track and almost impossible to reverse. One of the key pioneers of this new generation of ransomware attacks was the Reveton ransomware family around 2012,



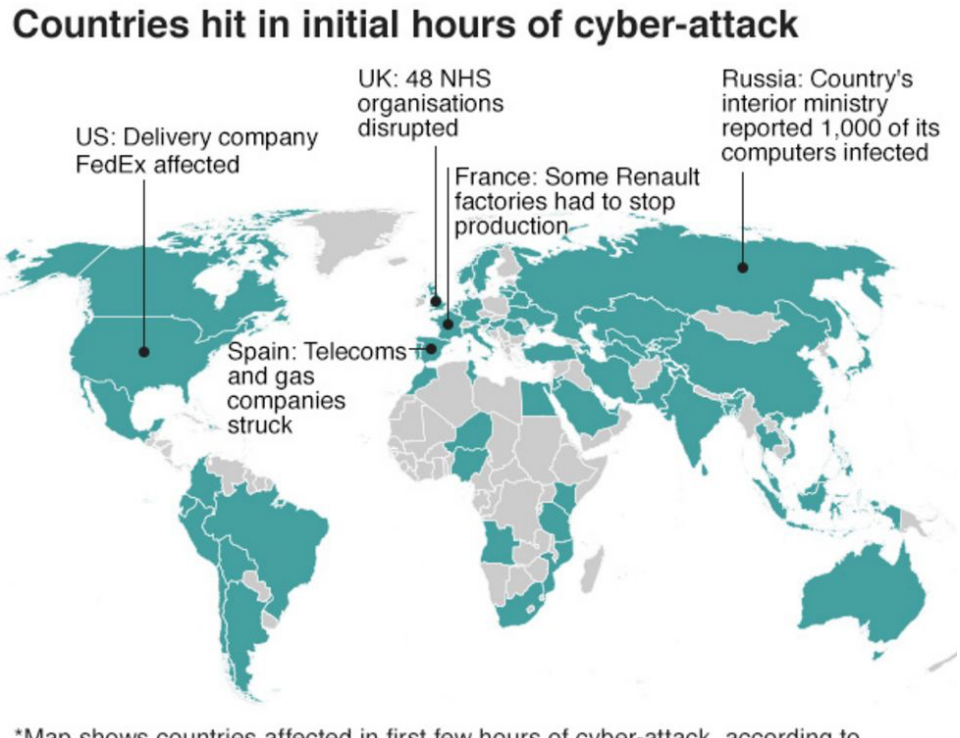
otherwise known as the “FBI-virus” (Harford). This family of ransomware would infect users through multiple mechanisms such as through compromised web links, installation packages, and outdated operating systems (Fouda). The ransomware would lock users’ computers with a “lock screen” stating that the computer had been locked by the FBI (or a national police bureau in other countries). The screen threatened that if the victims didn’t pay the fine, they would be arrested and subject to higher fines or even imprisonment. While earlier variants of the ransomware primarily used prepaid cards such as MoneyPak, later strains asked users to pay up in BitCoin (Lessing). Cryptocurrencies were ideal for ransomware, as threat actors could efficiently, anonymously, and irreversibly receive payments from victims (Harford).

In addition to being one of the most prominent early adopters of cryptocurrencies, the Reveton ransomware family was also the first widely available Ransomware-as-a-Service (RaaS), which, as stated earlier, dramatically lowered the barrier of entry for cybercriminals. As such, RaaS dramatically enlarged to scale and scope of ransomware attacks, modernizing it to be a profitable, efficient, and effective form of cybercrime. With RaaS and cryptocurrency payment being two hallmarks of modern ransomware attacks, it could be said that the Reveton ransomware family was crucial in setting the modern technical standards and practices for industrial-scale ransomware attacks.

WannaCry, 2017 – Global Institutional Targets with State-backed Actors

Though early attacks such as the Reveton ransomware family primarily targeted individuals and their personal devices, gradually ransomware began targeting more institutional targets, including company software systems and government systems. Targeting institutions could prove far more profitable than targeting individual users, as institutions often had significantly more financial resources and often the risks of "not paying up" for an institution were much higher than for an individual, as they often had cascading social repercussions. For example, if hospitals were unable to access patient data, this could dramatically hinder medical treatment and jeopardize patients' lives.

The WannaCry virus is one of the most famous examples of a ransomware of important institutions around the world, affecting over 200,000 devices in over 150 countries, targeting outdated Windows machines. This was an indiscriminate attack against both governments and private companies alike, from FedEx to the NHS ("The NHS Cyber Attack").



*Map shows countries affected in first few hours of cyber-attack, according to

Once WannaCry infected a victim's computer, it would encrypt the users' file disk and demand a series of ransom payments in BitCoin. If the victim did not pay within the specified timeframe, WannaCry would demand higher and higher payments as well as begin destroying users' files. Moreover, WannaCry was self-propagating; in addition to infecting a victim's computer, this "computer worm" would also search for other vulnerable devices on the infected computer's network, before sending those vulnerable machines an attack payload as well. This trait meant that WannaCry was uniquely suited to attacking institutional networks. On these networks, there are often thousands upon thousands of different devices connected to a single network, all running the same or similar operating system. Therefore, if WannaCry penetrated one computer on the network, it could potentially encrypt all devices on the system, thus disabling information backups stored on other devices and causing debilitating damage. The National Health Services (NHS) in the United Kingdom suffered immense damage due to the WannaCry ransomware. The UK's National Audit Office reveals that the NHS had not been adequately prepared for a national cyberattack scenario, and that "This meant the NHS was not clear what actions it should take when affected by WannaCry. NHS England found that responding to WannaCry was different from dealing with other incidents, such as a major transport accident" ("Investigation: WannaCry cyber attack and the NHS"). Because of this, doctors were unable to access any patient data, resulting in cancelled surgeries, appointments, and other operations. Thus, mass ransomware attacks such as the WannaCry virus may have catastrophic consequences on society-at-large, denying citizens essential services such as healthcare.

WannaCry is also an important case study to examine because it also exposes some political interests behind the use of ransomware and its implications in cyber-warfare. The backdoor exploited in the WannaCry attack was a Microsoft operating system bug known as “Eternal Blue Exploit” that allowed attackers could remotely execute code on a victim’s computer (“The WannaCry Ransomware”). This bug was discovered by the US National Security Agency (NSA), which kept it secret for over 5 years from both Microsoft developers as well as the general public. The NSA only informed Microsoft about the exploit after it faced a breach itself and knowledge of the exploit fell into the hands of a hacker group, the “Shadow Brokers,” ultimately resulting in one of the most disruptive cyberattacks in history (Nakashima).

This revelation raises several important questions concerning the interaction between intelligence agencies, system vulnerabilities, and ransomware. Should the NSA have told Microsoft about this exploit earlier, or should they hold on to it in order to gain profitable information from it? What about similarly powerful exploits? Should there be a threshold standard — an “ethical code of conduct” — intelligence agencies should use to evaluate whether or not to publicize a highly-potent exploit such as the “Eternal Blue Exploit”?

Another important political implication behind the WannaCry virus is the political affiliation of the hackers. Code within the WannaCry virus suggests a connection to the hacker group Lazarus, which some believe to be affiliated with the North Korean government. US Homeland Security Advisor Tom Bossert claimed in a Wall Street Journal article that “the US publicly attributes the massive “WannaCry” cyberattack to North Korea” (Bossert). As cyberattacks have become

increasingly sophisticated and cybersecurity increasingly tied with national security interests, there have been an increasing number of incidents where hacker groups are directly or indirectly affiliated with state-actors. Thus, when considering a policy proposal mitigating the negative social impact of ransomware, there are additional many political problems to be considered: how should we punish suspected state-actors? How do we define "affiliation" with a certain state? Should the United States retain offensive ransomware capabilities as a means to deter attacks? Should we treat ransomware the same way we treat nuclear weapons?

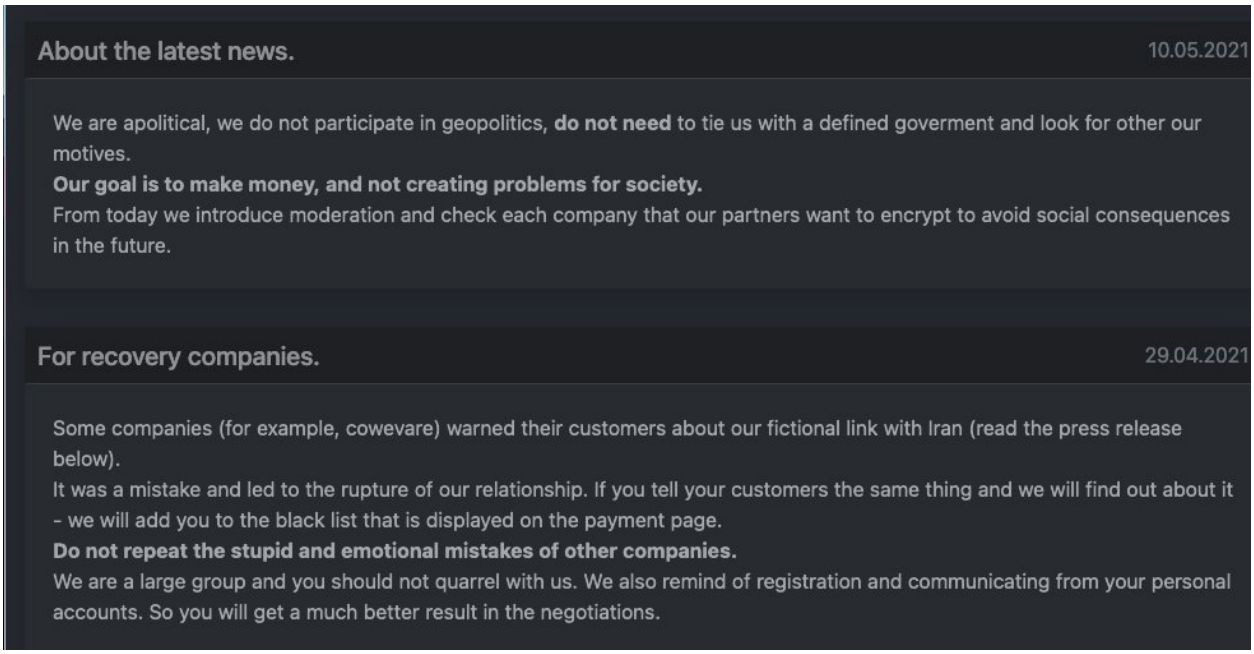
DarkSide, 2021 – The Colonial Pipeline Attack and the "Honorable Thief"

Ransomware recently returned to public attention after the widely publicized attack against Colonial Pipeline in May 2021. This attack was enabled by the software of the allegedly Russian-affiliated attacker group DarkSide, a group solely targeting large for-profit organizations (Patil). When attacking these targets, the criminals would threaten to make commercially sensitive data, such as technical specifications for a new product or the company's internal financial data and messages, publicly available. Publication of this sensitive data could result in dramatic revenue losses for a company and result in a publicized scandal. The hacker group DarkSide developed a Ransomware-as-a-Service with the same name, which caused the infamous Colonial Pipeline cyber-attack of May 2021.

According to Politico, the Colonial Pipeline ransomware attack was the "largest and most successful cyberattack on oil infrastructure" in US history (Gonzalez). With Colonial Pipeline

delivering about 45% of all of the US East Coast's fuel demands, it has been called the "jugular" of the US fuel pipeline system. The DarkSide virus infected the company's IT systems, and out of an abundance of caution, Colonial Pipeline shuttered its oil pipelines for a five-day period, from May 7 to May 12. According to Bloomberg, the attackers were able to gain access to over 100 gigabytes of data, which they threatened to publish. Thus, the attackers launched a double extortion scheme, asking Colonial Pipeline to pay for both the "keys" needed to decrypt the encrypted files, as well as for not publishing the proprietary data (Robertson). Ultimately, Colonial Pipeline paid $4.4 million dollars (75 bitcoin) in ransom for the decryption keys.

The social repercussions of the Colonial Pipeline cyberattack were tremendous. Four US states — North Carolina, Virginia, Georgia, and Florida — declared a statewide state of emergency, and gas prices spiked to $3 a gallon, a level not seen in the past seven years ("DarkChronicles"). Ironically, the social reaction was so severe that the DarkSide developers had to release a statement on their website clarifying that they simply developed the RaaS behind the attack and were not directly responsible for the attack. Rather, it was 'third-party' operators, and that "our goal is to make money, and not [create] problems for society," and that this incident prompted to conduct a background check on their business partners.



This denial of responsibility for the Colonial Pipeline attack also raises several interesting points that should be debated in crafting legislation to counteract ransomware attacks. Should the 'direct operator' and the RaaS service be held to the same level of accountability? Could we legalize the current RaaS market with government purchases to better understand cybersecurity flaws — turn these into "white-hat" hackers?

The Future of Ransomware –– Ransomcloud and the IoT

Ransomware approaches and targets continue to evolve as the digitized world evolves. Today, we are on the brink of two important technological revolutions: that of cloud services and of the Internet of Things (IoT). There are many public cloud service providers, such as Microsoft Azure, Amazon Web Services, as well as other Software-as-a-Service (SaaS) companies which have dramatically lowered the economic and technical costs associated with engaging users online. Many small and medium-sized businesses rely on these services to host websites and

engage with clients and customers, and often store crucial operational data in the cloud. The spontaneity, flexibility, and reliability of the cloud has persuaded large and small companies alike to move large amounts of previously locally stored data onto specialized servers in the cloud, especially since the global COVID-19 pandemic and "remote work".

The concentration of commercially and operationally valuable resources online means that the cloud represents a high-value target for future ransomware attacks. Security experts have suggested that "getting to the cloud data is the holy grail for attackers" (Glover). Thus, a new generation of ransomware targeting cloud services, ransomcloud software, is being rapidly popularized. Ransomcloud have three main variants, differing in their vectors of attack (Glover):

1. **Local attacks synced onto the cloud**: ransomware that first infects users' local machines, then spreading to the cloud through data syncs
2. **Cloud phishing:** phishing emails sent to cloud email accounts such as Office365, which then deploy phishing payloads to the cloud directly to encrypt all files on the organization's cloud server
3. **Direct service-provider attacks**: Ransomware that directly attacks the cloud service provider, which means that all of the cloud services' clients are unable to access their data. This variant is particularly effective and destructive. In 2019, a single ransomware attack on cloud service provider DDS Safe paralyzed over 400 different dentistry offices across the US.

In addition to targeting cloud data, future ransomware attacks are also likely to exploit vulnerabilities on the Internet of Things (IoT). From smart-watches to smart-fridges to smart-cars, our everyday lives are increasingly surrounded by IoT appliances, all capable of receiving, storing, and sending data on a network. In spite of the huge increase in everyday conveniences and "smart" functionality, without proper security measures, these IoT devices could be massively exploited. Your "smart home" could very easily turn into a "smart hell." Consider the following possibilities:

1. Smart vehicles sieged by ransomware that disables the braking system
2. Smart air-conditioning and fridges sieged by ransomware that releases toxic fumes
3. Smart burglar alarms, smoke detectors, home surveillance disabled by ransomware

It is no wonder that security experts have hailed the combination of ransomware and IoT devices as a "recipe for disruption." Often, IoT devices are not held to the same cybersecurity standards as computers or tablets, and thus are often the "weakest link in the chain" for a home network. Security researchers have successfully shown how a smart thermostat is able to be infiltrated with simple hardware hacks (Tierney). As the researchers note "Simple security controls would have stopped this hack working, yet they weren't present," and they would be able to set the temperature at will: to the maximum during summer, to the minimum during winter, until the user paid the ransom.

IoT ransomware attacks are not just limited to the "smart home"; industrial-scale machinery and infrastructure are also ripe targets for IoT ransomware attacks. The concept of Operational

Technology, or OT, loosely refers to all industry machinery that interacts with other machinery rather than with end users. This includes a broad category of assets, from machinery in oil refinery to mechanical arms on the production-line to nuclear reactors. An attack on OT assets could have cascading effects on the entire supply chain and consequences for wider society. The Colonial Pipeline case is a cautionary tale. Even though the DarkSide ransomware only breached the company's IT (information technology) systems, the company had to shut down the OT systems because they were afraid that if the ransomware spread to those systems, the damage and consequences were going to be far more severe. In recent years, there has been a general trend for companies to integrate their IT and OT systems, making it easier for ransomware and other forms of malware to spread from IT systems to controlling OT software.

Current Situation

Modern Ransomware Traits

Modern ransomware attacks and ransomware families revolve around several key principles:

1. **Ransomware-as-a-Service**, "off-the-shelf" software packages significantly lowering the technical barrier to entry for cyberattacks, discussed many times previously. RaaS is also the reason why there are several distinct "families" of ransomware related to one another
2. **Cryptocurrency payments,** efficient, hard-to-track, irreversible payments
3. **High-Value Targets**, often selecting specific institutions (businesses or governments) that can have large social impacts
4. **Multilevel Extortion**, through (1) locking victims' data, (2) publishing or auctioning stolen data, (3) orchestrating a denial of service (DDoS) attack on victims' networks and systems, (4) directly contacting business partners, investors, and stakeholders
5. **Network-based Attacks**, affecting entire network systems instead of a single computer, and able to delete backups from networks

Federal Enforcement and Legislation

Currently, the Cybersecurity Infrastructure and Security Agency, CISA, an office under the Department of Homeland Security, is the primary government agency overseeing national infrastructure cybersecurity. It is the self-described "quarterback for the federal cybersecurity team," established in 2018 to work across the public and private sector and defend critical national infrastructure assets against cyberattacks ("About CISA").

CISA lists 16 critical infrastructure sectors, each with its own mechanisms and plans to respond to a cyberattack. The 16 critical sectors are as follows:

Figure 4: List of 16 Critical Infrastructure Sectors identified by CISA

Chemical Sector	Dams Sector	Financial Services Sector	Information Technology Sector
Commercial Facilities Sector	Defense Industrial Base Sector	Food and Agriculture Sector	Nuclear Reactors, Materials, and Waste Sector
Communications Sector	Emergency Services Sector	Government Facilities Sector	State, Local, Tribal, and Territorial Government Coordinating Council
Critical Manufacturing Sector	Energy Sector	Healthcare and Public Health Sector	Transportation Systems Sector

At present, however, there is still a relative lack of federal mandates specifically targeted at ransomware and ransomware attacks. Researchers have suggested that there needs to be federal and congressional action to periodically update "cyber-hygiene" standards, especially with reference to the question of ransomware ("Combatting Ransomware", 39). As these policy advisors note, "Regulations and standards related to cybersecurity vary widely, and in most cases do not specifically address ransomware." A possible remedy to this situation would be to institute a private-public partnership council to periodically set minimum required standards, akin to the Payment Card Industry Security Council for credit cards.

Companies often lag behind in updating industrial control systems and other IT and OT systems because doing so would be costly and temporarily disruptive to business. Hence, often-times

they are using legacy software and hardware that can be easily exploited by hackers. As such, the government could consider subsidies and other aid to companies that upgrade their IT and OT systems, making it easier for companies to invest in more resilient and robust IT and OT infrastructure.

Lastly, the federal government can also consider ways to disrupt the ransomware business and profit model; as long as ransomware attacks are profitable for attackers (who often operate overseas with near impunity), they will continue to harass both individuals and institutions. One way to do this is through introducing legislation to prevent ransomware cryptocurrency payments, forcing over-the-counter cryptocurrency exchanges to face legal responsibilities similar to traditional financial institutions, and using financial incentives to persuade cryptocurrency exchanges to share data with law enforcement.

Finally, law enforcement agencies could think consider offensive strategies against ransomware infrastructure, RaaS service providers, and affiliates. After all, they also use assets such as servers and machines to distribute their own data. What if law enforcement offensively seizes these assets through cyberattacks and conducts cyber-asset freezes until they extract more information from these criminal syndicates? Ultimately, ransomware technologies in and of itself are just a tool, a digital equivalent of a knife or firearm; it is the actor that wields these tools that causes social repercussions, not the tools themselves.

Questions to Consider and Committee Tasks

Task

The overarching committee issue is stated as: *Measures to Prevent Malicious Ransomware Cyberattacks on Critical National Infrastructure and Industries: Developing a comprehensive* ***Ransomware and Infrastructure Cybersecurity Act***. This Ransomware and Infrastructure Cybersecurity Act is implemented at the federal level. By the end of debate time, the committee should have a draft resolution formatted in MUN-style, with preamble and operative clauses.

Points of Consideration

The following are points of consideration to aid with developing a comprehensive resolution. This is by no means an exhaustive list of all the points you may want to consider.

1. The issue of ransomware and infrastructure cybersecurity spans both the public and private sector. What would be the distinct roles of each, and how would they coordinate with one another? What is the specific role of agencies such as CISA in this?
2. How much should we regulate cryptocurrencies and their vendors to prevent exploitation by ransomware actors? How much should we rely on voluntary cooperation?
3. How should we deal with ransomware where the actors are operating abroad? This is an issue of international concern, particularly when some actors may be backed by adversarial nations.
4. Is it possible to convert some vendors of ransomware into “white-hat hackers” and national security assets?

5. How should law enforcement and intelligence agencies such as the NSA, FBI, CIA interact with the exploits that they have found? Should there be an ethical standard on how to use, store, and expose discovered vulnerabilities?

Additional Sources and Reading

Ransomware History and White Papers

TechTarget, The history and evolution of ransomware:
https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware

Sophos White Paper, Ransomware: The Cyberthreat that Just Won't Die:
https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-ransomware-the-cyberthreat-that-just-wont-die-wp.pdf

Group-IB White Paper, Ransomware Uncovered 2020-2021:
https://explore.group-ib.com/ransomware-reports/ransomware_uncovered_2020

Symantec White Paper, Targeted Ransomware:
https://symantec.broadcom.com/hubfs/Symantec-Targeted-Ransomware-White-Paper.pdf

Case Studies

Reveton
Microsoft Malware Encyclopedia:
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32%2freveton

SDX Central:
https://www.sdxcentral.com/security/definitions/case-study-reveton-ransomware/

WannaCry
BBC Report of WannaCry Cyberattack: https://www.bbc.com/news/world-europe-39907965

National Audit Office Investigation:
https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf

Arconis, The NHS Cyber Attack: https://www.acronis.com/en-gb/articles/nhs-cyber-attack/

Washington Post on NSA leaking the EternalBlue exploit:
https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

DarkSide
Politico report on Colonial Pipeline attack:
https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984

Bloomberg on stolen data:
https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

Qualys blog on DarkSide ransomware:
https://blog.qualys.com/vulnerabilities-threat-research/2021/06/09/darkside-ransomware

Kaspersky Labs on the Colonial Pipeline Attack aftermath:
https://ics-cert.kaspersky.com/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/#_Toc72509154

Ransomcloud and IoT
Tech Monitor on Ransomcloud: https://techmonitor.ai/technology/cybersecurity/ransomcloud

Pen Test Partners on smart-thermostat ransomware:
https://www.pentestpartners.com/security-blog/thermostat-ransomware-a-lesson-in-iot-security/

Ransomware Legislation Recommendations

IST Ransomware Task Force Report:
https://securityandtechnology.org/ransomwaretaskforce/report/

CISA Description: https://www.cisa.gov/about-cisa

Works Cited

"About CISA." *Cybersecurity and Infrastructure Security Agency*, n.d. https://www.cisa.gov/about-cisa. Accessed 21 Dec 2021.

"Combatting Ransomware." *Institute for Security and Technology*, n.d. https://securityandtechnology.org/ransomwaretaskforce/report/. Accessed 21 Dec 2021.

"Cyber-attack: Europol says it was unprecedented in scale." *BBC World News*, 13 May 2017. https://www.bbc.com/news/world-europe-39907965. Accessed 20 Dec 2021.

"DarkChronicles: the consequences of the Colonial Pipeline attack." *Kaspersky Labs*, 21 May 2021. https://ics-cert.kaspersky.com/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/. Accessed 20 Dec 2021.

Fouda, Amir. "Win32/Reveton." *Microsoft Security Intelligence*, 10 Jan 2018. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32%2freveton. Accessed 18 Dec 2021.

Glover, Claudia. "Ransomcloud: How and why ransomware is targeting the cloud." *Tech Monitor*, 11 Oct 2021. https://techmonitor.ai/technology/cybersecurity/ransomcloud. Accessed 21 Dec 2021.

Gonzalez, Gloria. "'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack." *Politico*, 8 May 2021. https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984. Accessed 20 Dec 2021.

Harford, Isabella. "The history and evolution of ransomware." *TechTarget*, 30 Oct 2021. https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware. Accessed 18 Dec 2021.

"Investigation: WannaCry cyber attack and the NHS." *UK National Audit Office*, 25 Apr 2018. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf. Accessed 20 Dec 2021.

Lessing, Marlese. "Case Study: Reveton Ransomware." *SDX Central*, 17 Jun 2020. https://www.sdxcentral.com/security/definitions/case-study-reveton-ransomware/. Accessed 18 Dec 2021.

Nakashima, Ellen. "NSA officials worried about the day its potent hacking tool would get loose. Then it did." *The Washington Post*, 16 May 2017.

https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html. Accessed 20 Dec 2021.

Patil, Yogesh. "DarkSide Ransomware." *Qualys Community*, 9 Jun 2021. https://blog.qualys.com/vulnerabilities-threat-research/2021/06/09/darkside-ransomware. Accessed 20 Dec 2021.

"Ransomware Uncovered 2020-2021." *Group-IB*, n.d. https://explore.group-ib.com/ransomware-reports/ransomware_uncovered_2020. Accessed 20 Dec 2021.

"Ransomware: The Cyberthreat that Just Won't Die." *Sophos*, n.d. https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-ransomware-the-cyberthreat-that-just-wont-die-wp.pdf. Accessed 20 Dec 2021.

Robertson, Jordan. "Colonial Hackers Stole Data Thursday Ahead of Shutdown." *Bloomberg*, 8 May 2021. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown. Accessed 20 Dec 2021.

"Targeted Ransomware." *Symantec*, n.d. https://symantec.broadcom.com/hubfs/Symantec-Targeted-Ransomware-White-Paper.pdf. Accessed 18 Dec 2021.

"The NHS cyber attack." *Acronis*, n.d. https://www.acronis.com/en-gb/articles/nhs-cyber-attack/. Accessed 20 Dec 2021.

Tierney, Andrew. "Thermostat Ransomware: a lesson in IoT security." *Pen Test Partners*, 8 Aug 2016. https://www.pentestpartners.com/security-blog/thermostat-ransomware-a-lesson-in-iot-security/. Accessed 21 Dec 2021.