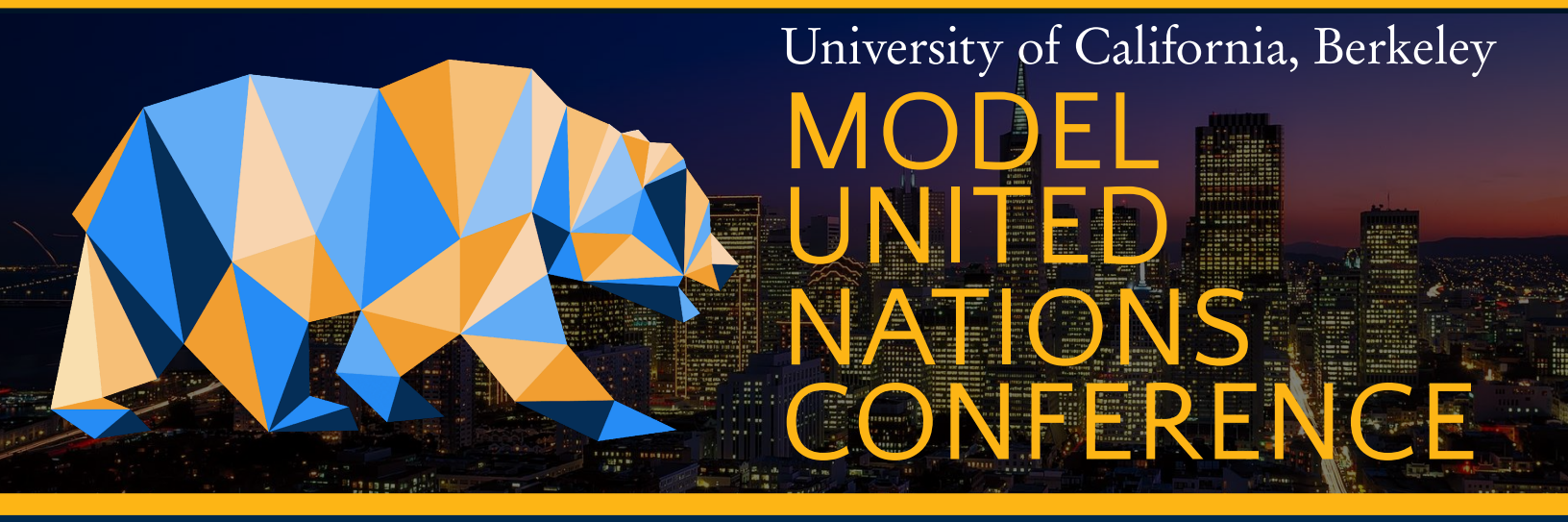
United States Senate

Data Privacy



XXV

Parth Nobel
Antonio Kobe Lopez

Contents

1 Letters from the Dias

Senators!

Welcome to UCBMUN XXV! I'm excited and honored to continue serving as a Chair for my fourth and final UCBMUN. I joined Model UN in the Fall of 2017, as a Freshman looking for a fun and friendly community at UC Berkeley. I could not have been happier with what I found. I traveled with our Model UN team throughout my time in college, and have at various points been UCBMUN's Secretary, Director of Technology, Speech Coach, an inaugural member of our Diversity and Inclusion Committee, and, early in my time at Cal, an Assistant Crisis Director. I've poured endless hours into planning for meetings, interviewing potential new members, advocating for improved funding, designing name tags and placards, finding typos on the printed placards, frantically running to the print shop to reprint placards, designing and building the old conference website, triple-checking the awards powerpoint for typos, frantically corralling a team to the airport for a 6AM flight, arguing about what font we should use for background guides, yelling "louder" at a nervous delegate during their first speech training, explaining voting bloc to high schoolers as I chair their first conference, and getting lunch with friends after Sunday awards stunningly happy, but delirious from having not slept. I'm excited to move on to the next phase of my life, graduate school in Electrical Engineering.

Data Privacy has fascinated me since I was a small child. In middle school, I could rattle off open questions on 4th Amendment law, and make comments about Louis Brandeis's *The Right to Privacy*. As I got older, I actually learned what I had been talking about. Trying to answer questions about this area has always captivated me and been a major part of what draws me back to policy and politics as I delve deeper and deeper into technology. I hope that senators who are familiar with the questions before us bring experience that helps us shape our answers, and I hope that those of you who learn about the area from this document discover why I find it so captivating and become inspired to dig deeper into it.

Lastly, Kobe and I would like to thank our Chief of Staff Emma Lapinsky for her rapid and substantial editing and Ryan Lehmkuhl for consulting with me on cryptography. I would like to personally thank Kobe for all his hard work and dedication in putting this committee together.

Sincerely,
Parth Nobel

Senators,

I am honored to welcome each and every one of you to UCBMUN XXV! Working to prepare this committee with Parth and the rest of our wonderful staff has been a great experience. Committees like this one, that allow us to partake in serious discussions about issues that affect us all, are places that not only allow us to take on the issues at hand, but also to interact with peers that we might not normally have the chance to. It is easy to forget the incredible nature of experiences that bring us together. In all the things I've been a part of, from sitting with school boards, editing videos for the school paper, coordinating cultural performance events, and even to a brief stint in acting, I've often forgotten to remember just how lucky I am to be meeting so many incredible individuals with their own stories to tell.

Technology plays a critical role in our daily lives and in how many make their livelihood. Take for instance this very conference, I suspect that you are reading this background guide through the screen of your personal computer, a computer connected to the internet and that has likely interfaced with an innumerable amount of servers and users in simply the last few hours. I myself have used the services of a number of video conferencing softwares and messaging systems while working on this guide and visited countless websites in order to collate the information you will read below. Staying safe in the digital age is no simple thing; corporations like Apple take pride in using their encryption and other protections to ward off digital criminals and other unwanted parties, while some governments attempt to pass regulative legislation like the GDPR in order to ensure accountability from those same corporations— but how sure are you that even governments have your best interests in mind? There is a huge amount of complexity at the heart of every argument to be made and it becomes even more complicated with the realization that technology will continue to evolve, likely to a degree we cannot foresee. This is the kind of difficulty and nuance that our committee will have you contending with.

As I end this letter, I want to offer a last round of appreciations and acknowledgements. To Parth, I send my deepest gratitude for working with me through this process and his dedication to this committee, as well as my apologies for all the late nights he has spent working on it. My most sincere thanks to our Secretariat, especially Rithika, Pranav, Sharicka, and Emma, for your dedication. As to you, the senators, I eagerly await seeing you in action and wish you the best of luck!

Cordially,

Antonio Kobe Lopez

2 Committee Logistics

2.1 Agenda

As American lives are increasingly digital and—therefore—connected, the question of how traditional notions of privacy translate to this domain have become increasingly important. Congress addressed some of these questions at the very beginning of the digital era, but many of those laws contain huge disconnects between Congress's original intent and the laws' impacts on modern technology.

There will be only one item on our agenda: drafting a bill to preserve and protect the data privacy of American citizens. This debate will begin on Friday morning and conclude with a Saturday afternoon vote on the drafted bill or bills.

The US Senate does not write policy in a vacuum. Throughout debates on pertinent issues, Senators face a shifting political landscape from scandals breaking, NGOs releasing studies, or the House or President declaring an extreme negotiating posture.

Accordingly, there may be interruptions during the committee introducing current events that make possible solutions untenable, such as the President threatening to veto any bill that includes public-private partnerships, or a scandal, such as *Motherboard* revealing that a major tech company is selling photographs uploaded to their photo backup service, that forces the Senate to consider expanding privacy protections.

2.1.1 Topics Excluded from this Debate

To help you target your research, the Dias wishes to highlight the topics that are **not relevant** to this committee, but which often appear in this space. **Senators are not expected to address these issues**. If you encounter any of these topics in your research, feel free to move along **without engaging with them, as they are not part of this committee**:

- Social media platforms liability for user-generated content. This is often discussed as the meaning of and what amendments should be made to Section 230 of the Communications Decency Act.
- Social media platforms policies and practices on limiting speech on their platforms.
- Broadband access. Neither the definition of broadband nor its availability and quality are relevant to this debate.

- Cybersecurity of government or corporate systems.[1]
- Content filtering for copyrighted content i.e. piracy. We do not concern ourselves with preventing copyrighted content from being distributed illegally.
- Net Neutrality and other consumer internet regulatory regimes (such as the Title II classification of ISPs debate).[2]
- The laws of war.
- Cyber espionage.
- US policy on state-to-state cyber activities.

2.2 Position Papers

Every Senator is required to write a paper outlining their views on the policy issues laid out in this document. **Senators are not encouraged or expected to elaborate on original research, beyond what they require to construct their solutions.** Senators are strongly encouraged and expected to address every policy issue raised in Section 6.5. In regards to formatting, please follow the UCBMUN Position Paper Guidelines. Please note that the UCBMUN Position Paper Guidelines require 1 page per topic and that Privacy from Government and Privacy from Megacorporations are considered separate topics for the purpose of determining page count. Your final position paper should be two pages.

2.3 Committee Procedure

United States Senate: Data Privacy will follow the UCBMUN XXV Rules of Procedure, subject to modifications presented in Appendix A.

[1] It may be necessary to address many questions relevant to securing consumer data from hackers or to impose some form of regulatory regime to enforce reasonable security practices; however, Senators are not expected to or required to prepare comprehensive security proposals, and the Dias discourages Senators from going too far into the weeds on this policy area.

[2] Our debate can, and probably should, include some discussion of ISP practices regarding monitoring consumer internet traffic, but not on the regulatory regimes the FCC uses to classify broadband or on how ISPs censor or favor content.

3 Digital Privacy

American law has long created two distinct areas where citizens receive, or at least expect, "privacy". We will summarize them in this document as Privacy from Government and Privacy from Megacorporations.

Many of the issues encompassed by Privacy from the Government fall into two umbrella questions: what data can the government legally obtain and how the government actually obtains that data. Obtaining data can be broken down into two pieces: the law enforcement question—what data can the government access while investigating a particular citizen for a particular crime—and the national security surveillance question—what massive volumes of data can the government sweep up indiscriminately while surveilling foreign targets. While the Bill of Rights places some limitations on the data the government can access while investigating citizens, the "third-party doctrine" leaves most digital data unprotected constitutionally.[3] Accordingly, the Senate can and should protect the rights of Americans beyond the minimum requirements of the US Constitution.

Some Americans, when discussing Privacy from Megacorporations, correctly assert that consumers have little to no rights in this space, as this is fundamentally a question of the contract the consumer agrees to with the Megacorporation. Most of the time the "contract" in question is a Terms of Service and Privacy Policy that no one reads, save the lawyers who drafted it. Congress, however, has the power to regulate the content of these contracts, banning certain practices, requiring other practices, placing legal obligations on one party, and allowing for enforcement beyond what the contract provides. This is the power that this Senate is called upon to use in this session.

[3]The Supreme Court has begun to change this reasoning, notably in the recent *Carpenter v. US* decision. Change, however, is slow to come and may not be particularly comprehensive.

4 Privacy from Government

4.1 Constitutional Rights[4]

One of the core features of American criminal law and its judicial system is the idea that the government faces limitations in how it investigates crimes and what evidence it is ultimately allowed to present in a criminal trial. These rights translate into key limitations on the power of government as they investigate criminals. In general, a given action can fall into one of three buckets: always legal, legal if (and only if) the government convinces a judge to issue a warrant, and always illegal. There are often caveats, exceptions, and special cases for all three buckets. For example, an officer may enter a house while in direct pursuit of a criminal without a warrant, but would otherwise need a warrant. In digital scenarios, however, these more complicated rules generally don't appear. Further, the standard of evidence required to get a warrant is generally "probable cause", which is a relatively high standard. The details of this standard are not particularly relevant to this committee.

The natural follow-up question is, "what determines where each action falls?" The answer is two-fold: the Supreme Court has declared that the Constitution protects some rights placing them in either the "requires a warrant" or the "never legal" category and Congress has passed laws prohibiting some actions and mandating a warrant for others. Senators are charged in this session in part with expanding protections beyond the basic Constitutional protections in digital contexts.

The Supreme Court's 4th Amendment jurisprudence, prior to *Carpenter*, does not require much in the way of warrants for the government to access digital data in the modern world. Not because technology fundamentally has different protections, but because the way consumers use technology in this cloud-centric world entails passing sensitive information to third parties. The Supreme Court has long held that once data has been surrendered to a third party, the user doesn't retain any privacy rights over the data, and therefore the government does not require a warrant to access the data.

Under 2018's *Carpenter*, there is a new standard for what third-party data can be obtained without a warrant: it seems to rest on the question of how much data is the government obtaining and whether giving the data to the other party is particularly

[4]This section glosses over huge amounts of nuance, strange and difficult-to-reconcile exceptions, and much much more. It will, hopefully, make for a reasonable introduction.

intentional. This standard is fairly ill-defined and it is not clear how to apply it to anything other than the specific facts it arose from.

In some areas of digital privacy, the law is largely incomprehensible and wildly inconsistent across states.[5] As such, the Dias recommends assuming that protections under the new standard are minimal and Congress should aim to protect what it wants protected through legislation.

4.2 Limits to Law Enforcement Data Collection

4.2.1 Data Stored Abroad

In general, and especially in the United States, the internet is global; data stored in Ireland is as accessible to an American user as data stored in an American data center.[6] In a case beginning in December 2013—before being mooted in 2018—Federal investigators attempted to gain access to data stored by Microsoft on Irish servers, under the Stored Communications Act. The FBI attempted to use the 1968 Stored Communications Act to have a court issue a warrant requiring Microsoft, in the US, to pull data stored in Ireland to the US and then hand it over to the government.

The question at the core of the case: Do US courts have the power to compel American corporations and individuals to retrieve data stored on foreign servers?

While SCOTUS was deliberating on the issue, Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act which clarifies that courts do have the power to compel American corporations and individuals to fetch data from abroad. It, however, includes a careful carve-out exempting parties from producing the data if it requires them to break laws in the foreign state.

The U.S. solution to governmental access of corporately owned data is far from the only existing solution. Russia's data privacy concerns, and more critically domestic surveillance goals, have led them to require the storage of all data on Russian users on Russian servers. Russian data localization legislation provides enhanced power to its

[5]For an example of an area where many questions are still unresolved see Kerr, Orin. "The Law of Compelled Decryption is a Mess: A Dialogue." *The Volokh Conspiracy*. 8 Aug. 2020, https://reason.com/2020/08/10/the-law-of-compelled-decryption-is-a-mess-a-dialogue/.

[6]Obviously, the speed of light and, far more significantly, limitations in technology require that the further a server is from the user the longer it takes for initial access and to conduct synchronous communication; however, for most use cases (*e.g.* not video streaming where a massive volume of synchronous communication occurs perpetually), those slowdowns are trivial and smaller than humans can perceive them.

government; allowing Russia to easily censor, shut down, or surveil the data of any of its citizens. The requirement of a physical presence of servers can be viewed as a form of economic protectionism. The requirement also creates a large barrier for foreign companies entering a marketplace, especially since Russia has enforced their data localization laws by banning services such as LinkedIn for failing to comply.[7] [8]

In this session, Senators should feel free to reopen this debate and decide if they want to preserve the existing exceptions or if they want to approach the issue differently.

4.2.2 Stored Communications Act

The Stored Communications Act of 1986 was passed in response to the development of new technologies, which might lack 4th Amendment protections, potentially allowing law enforcement to avoid existing requirements to obtain a warrant.

To fully understand the decisions that went into writing the law, let's consider the state of email and computing in general in 1986. First, storage is expensive, email servers cannot store endless amounts of documents, certainly not extended histories of every email sent and received by their users. Second, users did not expect the same data to be synced across multiple computers, *i.e.* email does not need to be synced between the user's Personal Computer and their work computer.[9] Second, the primary way to access email is with a protocol called "POP" or the Post Office Protocol.[10] POP works (very roughly) by a user logging into the email server, downloading the emails, then telling the server they received them, and the server then deleting them.[11] When Congress drafted the SCA, *it was common practice to delete every email from the email server after it was opened and for the server to never store sent emails.*

In this context, the SCA provides the highest degree of protection to emails that have been sitting on a server for less than 180 days and which have never been accessed by the user. To compel access to these emails, law enforcement needs a warrant. Further,

[7] "Moscow Court Upholds Decision to Ban LinkedIn in Russia." *The Moscow Times*, 10 Nov. 2016, https://www.themoscowtimes.com/2016/11/10/moscow-court-upholds-decision-to-ban-linkedin-in-russia-a56086.

[8] Sayer, Peter. "LinkedIn Blocked by Russian Government." *PCWorld*, 17 Nov. 2016, https://www.pcworld.com/article/3142500/isps-ordered-to-block-linkedin-in-russia.html.

[9] In modern times, users expect simultaneous access to all of their emails from their cell phones, tablets, work computers, and any other device they're using.

[10] Modern email clients rely on IMAP, proprietary protocols, or a more modern version of POP.

[11] See RFC 918. In RFC 937, which introduces POPv2, it becomes possible to download email and mark it read without deleting it.

providers can only voluntarily share this data with law enforcement if there is an urgent "emergency involving danger of death or serious physical injury".[12] If, however, the data has been sitting on the server for 180 days or had been accessed and left on the server, then the protections are far more minimal and do not even begin to approach the burden of a warrant. In the drafters of the SCA's then-accurate understanding of technology, this was unusual! They thought that everyone would download their emails when they read them and then delete them off the server and that everyone would check their email at least every 6 months. Thus, they believed, only abandoned email inboxes would be accessible without a warrant under this statute.

The assumptions Congress made when it passed the SCA have been fundamentally undermined by modern technology. Most email users rely on some form of webmail, such as GMail, Yahoo! Mail, Microsoft's offerings in this space, or Apple's iCloud email.[13] These services encourage users to keep their emails on the provider's server at all times. Users are expected to keep their opened emails on the server and to store years upon years of archival emails on the server. *All of these emails lack the strong protections that Congress had intended to provide American citizens' emails with when they passed the Stored Communications Act in 1986.*

Congress has made some efforts to improve the situation in other areas where the SCA applies, but email continues to have a huge disconnect between Congressional intent and the rights protected in practice today.

4.2.3 Foreign Intelligence Surveillance

Originally passed in 1978, the Foreign Intelligence Surveillance Act outlined the government's legal limits in foreign intelligence collection and attempted to establish protections for American citizens. Since its implementation, FISA has seen a number of amendments and changes, especially in the wake of the 9/11 attacks, that have expanded the operating power of the NSA and its data collection programs. Section 702 of FISA, Executive Order 12333, and the Patriot Act are all notable examples of legislation that expanded NSA powers and have faced criticism for their allowance of collection of American citizens' data

[12] 18 U.S.C. § 2702(b)(8).

[13] The Dias doesn't name Microsoft's products because, to be frank, the Dias is deeply confused on their branding. Is Outlook their provider-independent mail software? A website users can use to access a Microsoft-server backed mailbox? Is Microsoft 365 the cloud service which the email comes with? The Dias didn't think it was worth their time to make sense of it, and is deeply skeptical it is possible to make sense of.

through unintentional (according to the NSA's outward facing offices) and warrantless collection methods.

One critical component of FISA is its creation of the Foreign Intelligence Surveillance Court, commonly known as FISC or FISA Court. Typically, a request to surveil a domestically located target must be filed as a FISA application and sent to the FISC for approval. FISC is supposed to primarily verify that the surveillance does not directly target US Citizens and that precautions are taken to make the accidental inclusion of a US Citizen improbable.[14] From the time of the act's passing in 1979 to 2006, just under 23,000 applications had been filed and only 5 had been rejected. However, in recent years the number of rejections has risen considerably.[15] Due to the nature of the FISA Court, most applications are classified, so only the number of applications is publicly available information.

Since it's initial passing FISA has seen a number of amendments. Section 702 was added as a part of the FISA Amendments Act of 2008. It expands the potential targets of FISA surveillance to any foreign national located abroad, and allows the government to access US providers of internet-based services like Google or Facebook to carry out such surveillance.[16] While Executive Order 12333 does not explicitly alter FISA, it's mandate that data be shared within the intelligence community and its "authoriz[ation] to collect, retain or disseminate information concerning United States persons" does allow the bulk collection of American citizens data within certain bounds.[17] In the aftermath of the September 11th attacks, FISA received a sent of amendments as a part of the Patriot Act. Section 215 of the Patriot Act amended FISA by allowing the NSA to collect telephone metadata, including the time of a call, its duration, and the participating phone numbers. This warrantless direct collection of cell phone information was stopped when Congress passed the USA FREEDOM Act in 2015. The USA FREEDOM Act required cell phone companies to store this metadata, and allowed the NSA to gather the data from the companies only after obtaining a warrant from the FISA Court. Section 215 expired in

[14] "Foreign Intelligence Surveillance Court (FISC)." *Electronic Privacy Information Center*, https://epic.org/privacy/surveillance/fisa/fisc/.

[15] "Foreign Intelligence Surveillance Act Court Orders 1979-2017." *Electronic Privacy Information Center*, https://epic.org/privacy/surveillance/fisa/stats/default.html.

[16] "Section 702: What It Is & How It Works." *Center for Democracy and Technology*, https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf.

[17] Joel, Alexander. "The Truth About Executive Order 12333." *Politico Magazine*, 18 Aug. 2014, https://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121#ixzz3AqBJoNHn.

May of 2020, and, as of August 2020, remains expired.[18]

The ability for the government to collect information seemingly unilaterally along with a lack of transparency has drawn criticism from a wide range of persons and organizations. On June 6, 2013, *The Washington Post* and *The Guardian* reported on leaked documents provided to them by a former NSA contractor detailing a number of NSA programs conducted under the authority of FISA Section 702. The documents showed the public that the government's surveillance methods were much wider reaching than previously understood. This sparked a wave of criticism by the public and elected officials alike.

Debate over FISA and its related legislation continues, some relating to legality, others regarding efficiency, and others on the ethical ramifications. Civil liberties organizations such as the ACLU argue that FISA is unconstitutional because it breaches personal privacy, especially since American's data can be collected outside the context of a criminal investigation. At its core, FISA asks how the United States should balance systemic security and personal privacy. The status quo leans heavily towards systemic security.

4.3 Obtaining Lawfully Collectible Data

4.3.1 Cryptography

Cryptography is a broad field covering a huge area of mathematics, including the mathematical discipline of securing and verifying data. Even this subfield is vast and stunningly complicated; however, for the topics on hand, we can apply some major assumptions and sweep away thousands of academic papers and decades of research to describe cryptography as providing four key abilities when building computer systems:

- Securing data so that only a particular computer can access it and so that the data can't be tampered with.
- Securing data so that only those who know a password can access or modify it. This is often used to secure phones and other computers from tampering if someone other than the owner has access to them.
- Allowing two computers to communicate with each other in such a way that no one who overhears the communication can understand what they're saying.

[18]Li, Katniss. "Section 215 of the Patriot Act Expected to Sunet in December." *Harvard Journal of Law and Technology*, 28 Oct. 2019, https://jolt.law.harvard.edu/digest/section-215-of-the-patriot-act-expected-to-sunset-in-december.

- Allowing digital documents to be "signed" by a particular computer. Well-known entities, such as the government or major corporations, like Apple and Google, tend to have these special computers that are known to be associated with them. This allows us to say that a document has been "signed by Apple." A signed document cannot be modified without removing the signature, but the document, with its signature, can be perfectly copied and distributed by any party who has a copy of it.

The computers used in the last bullet are often specialized, containing a "Hardware Security Module" (HSM). A HSM is a part of a computer that contains all the data required to create the digital signatures. They are designed to be impossible to physically open without destroying the device. If someone has physical access to the HSM, they can only steal the physical HSM (which will presumably set off alarms) and any attempt to extract the data will destroy the device. Computers with HSMs are sometimes kept disconnected from the internet and other networks to try to prevent remote hackers from being able to access them, and are almost always kept in locked rooms or vaults.

To understand the challenges that cryptography poses to law enforcement's efforts to access lawfully-collectible data, we turn to a well-known case study. In the wake of a domestic terrorist shooting in San Bernardino, CA in 2015, the FBI called upon Apple to provide assistance in unlocking the iPhone belonging to the late murderer. The Apple-designed encryption on the murder's iPhone made it very difficult for the FBI to access the contents of the device. Notably, the iPhone had a feature that would destroy all data on the phone if more than 10 incorrect password attempts were made. The FBI was asking Apple to disable this protection, which would have allowed the FBI to try all possible passwords. (This technique of encryption breaking is commonly referred to as "brute forcing", and is normally not feasible; this case was special because the murderer had used a 4 digit passcode). Tim Cook, CEO of Apple, referred to the request as "chilling" and likened it to asking for a master key to every Apple device manufactured. Apple declined to help the FBI. The FBI argued that complying would be a one-time rendering of assistance with no long-term consequences for Apple. Tech firms supporting Apple's refusal to assist argued that the existence of such a master key would be a lasting and exploitable weakness in data security for all of Apple's products. The FBI then attempted to have a court compel Apple to comply with their request; however, before the court ruled, the FBI had begun the process of accessing the phone with the help of a third-party vendor and gained access. As the case was now moot, the court dismissed the dispute with the consent of all parties.

Figure 1: This clean room, found in the NanoLab at UC Berkeley, contains some of the precision equipment that would be needed to disassemble the iPhone and connect the memory chip in the phone to a custom-built computer that allows for the extraction of the data. The process would destroy the phone, and any mistakes would destroy all the data without extracting it.

A number of questions remain about how the FBI gained access to the iPhone's content. Who was the third-party vendor? How did they manage to unlock the iPhone? The only publicly available answers are based exclusively on speculation. The two most likely methods the third-party vendor used to gain access to the phone are either through the discovery and exploitation of a new security vulnerability in the iPhone's data security systems, or through the physical deconstruction of the phone in order to gain access to the data storage components. Once the data storage components are extracted, they can be attached to a custom built computer that allows for brute forcing the password. Both methods would be incredibly expensive. The second method always destroys the iPhone and has a high risk of destroying the data without recovering it. Public information confirms that the FBI spent approximately one million dollars to gain access to the phone's content.[19] Subsequent media reports strongly imply the FBI's secret contractor used the second option, risking destroying the data had any mistakes been made.

Let's disassemble all the moving pieces here. First, the FBI unambiguously had the legal authority to access the contents of the phone. However, the data on the phone was

[19]Hosenball, Mark. "FBI Paid Under $1 Million to Unlock San Bernardino iPhone: Sources." *Reuters*, 28 Apr. 2016, https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032.

inside a secure vault and, unlike the physical world, where the FBI can either lockpick or use dynamite to open any vault, it is mathematically impossible to open the vault without the combination. Further complications arise in the way the iPhone is built; it is impossible to access the vault directly. The only way for a user to attempt to access the contents of the vault is to give an attendant a possible combination and have the attendant go try the combination and then come back.

The attendant only obeys instructions it can mathematically prove were, at some point in time, approved by Apple. The attendant cannot speak directly with Apple to verify either that the instructions are up-to-date or that a given instruction is only to be obeyed by the attendant for one particular iPhone. It can only verify that Apple, at some point, "signed" the instructions it receives. Apple currently has only signed instructions that say "if you [the attendant] are given 10 incorrect guesses, destroy the contents of the vault."

The FBI asked a court to require Apple to write and sign instructions to the attendant that say "allow an unlimited number of combinations to be tested as rapidly as you [the attendant] can check if they are correct." Anyone who has a copy of these signed instructions (it is impossible to prevent the creation of perfect digital copies) can present it to an iPhone and then guess every possible password, which for the traditional 4 character numeric password, would take at most 3 hours to find the password. The FBI would then present these instructions to the specific phone they're targeting and guess the password. *These instructions can be presented to any iPhone and it is* impossible *to use technology to prevent someone who has access to a copy of the instructions from making a perfect copy of them.* To be clear, anyone—from a renegade agent, a foreign spy working in the FBI, a hacker who has hacked into the FBI's computer systems, or an honest agent who is misled by a social engineering campaign—with access to the instructions could leak them, *and destroy the security of every iPhone on the planet.*

4.3.2 Compelled Password Disclosure

Consider the case where a user has never transmitted data or given it to a third party and instead has used cryptography to create a hard disk with their data which cannot be unlocked without their password. In the physical world, this is analogous to a suspect keeping a safe in their basement with their data. Similar to the case above, the FBI in the physical world would pick the lock.

Demanding that manufacturers unlock these devices, as the FBI did in the previous

section, isn't an option here. The passwords are too large and too complicated for attempts at brute forcing to succeed. Often brute forcing is already available, but infeasible to use. The only option is then ordering the owner of the device to provide the password themselves. Some courts believe that they can compel the owners of devices to unlock them, others believe they can compel owners to give up the password itself.[20]

In 2015, a Philadelphia man accused of owning child pornography had his laptop seized. Police forensic analysis indicated the computer had been used to download the illicit files and store them on two encrypted external hard drives. When compelled by the court to decrypt the hard drives, the accused man claimed to have forgotten the passwords, and was subsequently held in contempt of court and was imprisoned.

The man challenged his imprisonment by calling upon his Fifth Amendment Rights against self-incrimination, arguing that unlocking the drives would be proving that he owned them and any content on them. The court rejected this argument, holding that the government already had evidence of his ownership of the drives; however, the man made a second challenge to his imprisonment that hinged upon a 1970 federal statute limiting imprisonment to 18 months for witnesses that refuse to testify. The 3rd Circuit held that this statute's limitation applies to all legal proceedings, not only formal trials. The man could therefore only be held for 18 months for failing to produce the password.

On one hand, sometimes people have forgotten their passwords. Should they really be imprisoned for 18 months? This is especially concerning in cases where a witness may not have committed any crimes, but the police believe they control devices that contain evidence of crimes. These witnesses have no Fifth Amendment rights and, therefore, can be imprisoned for not remembering a password.

On the other hand, consider an accused person who is withholding evidence of a crime which almost surely will lead to a sentence much longer than 18 months. If the government has no other way to prove they committed the crime, then should the accused be able to escape with just 18 months in prison? Some argue that the government will almost surely be able to find other evidence if the person is actually guilty and therefore this question has a faulty premise.

Further, The 3rd Circuit opinion makes no distinction between failing to testify and failing to provide a password (and therefore access to a body of evidence). It is not clear

[20]Professor Orin Kerr, a leading scholar in this space, covers the giant question mark around the 5th Amendment and compelled disclosure quite humorously here: Kerr, Orin. "The Law of Compelled Decryption is a Mess: A Dialogue." *The Volokh Conspiracy*. 8 Aug. 2020, https://reason.com/2020/08/10/the-law-of-compelled-decryption-is-a-mess-a-dialogue/.

these are analogous situations. It is not clear that Congress intended to adopt a universal 18 month limitation on all witnesses failing to comply with a Court order. Finally, Congress almost surely didn't intend this policy to apply to accessing the volume of data that an encrypted hard drive or phone may contain.

4.3.3 Going Dark to Hackers, and the Government

Let's go back to our list of things cryptography allows, specifically, how cryptography allows two computers to communicate such that no one who overhears the communication can understand what the computers are transmitting. This falls into two categories: 1. the benign encryption called "transport-layer security" used to secure communication between consumers and their banks while they're browsing the web; 2. end-to-end encryption used to allow two consumers to communicate securely with each other over third-party-controlled servers. End-to-end encrypted texting products on the market include Facebook's WhatsApp, Facebook's "Secure Conversations" in the mobile version of Facebook Messenger, Apple's iMessage, and, the Dias's recommendation for all communication, Open Whisper Systems's Signal.

In the phone call and video space, end-to-end encrypted offerings include Google's Duo, Apple's Facetime, Microsoft's Skype, and, the Dias's recommendation, Open Whisper Systems's Signal.[21] The benefits of these systems are incredible: Hackers can breach the servers of the systems providing the service without gaining any of the most valuable assets, the user communication. This greatly reduces the economic benefits for hackers of attacking these services and almost surely reduces the cost of defending these systems.[22] They create an incredible challenge for law-enforcement though. Law-enforcement, armed with a valid warrant, cannot demand that third-parties hand over old communications or wiretap continuing or future communication.

Law enforcement brands the use of technology that is immune to wiretapping as the users of the service "going dark" to their investigations. They argue that the prevalence of

[21] Unrelated to the topic of this committee, the Dias recommends using Open Whisper Systems's products for all secure communications in your life for a litany of reasons: OWS is a non-profit and not in the business of selling your data; they are significantly more featureful then the other secure offerings; their explicit purpose and goal is to ensure the privacy of their customers; their protocols are the gold-standard for end-to-end encryption; their implementations are open-source and regularly audited; and they do not attempt to lock their customers into buying expensive and, arguably, deeply overpriced devices in order to retain access to their communication channels.

[22] Wagner, David. "Principles for Building Secure Systems." *CS 161 Lecture Notes*, UC Berkeley, https://cs161.org/assets/notes/Principles.1.19.pdf.

US consumers using secure communications to ensure that their data is harder for criminals to access, also means that other criminals have an easier and safer time coordinating and planning their criminal activity. Originally, law enforcement largely described encryption as a tool used by not just US consumers, but by terrorists planning and coordinating attacks.[23] After years of unsuccessful attempts to depict this as largely an issue in terrorist cases, the law enforcement community has shifted to talking about how encryption enables the distribution of child pornography and similar criminal and vile media.[24]

The technology community has generally rejected law enforcement's dire views of encryption. Their main objection is that encryption is available and there's no feasible way to prevent people from using it. The best Congressional action could hope to achieve is to make it harder to access or to criminalize encrypted systems. Criminals could easily gain access to software with strong encryption and then use that to still safely communicate or distribute unlawful media. Congress's inability to stop the illegal distribution of copyrighted material is a clear indicator of the hopelessness of stopping the distribution of strong encryption implementations. Further, encryption is a necessary part of securing the data of American corporations and citizens. Ensuring that a citizen who has their phone stolen doesn't have criminals gaining access to all of their personal photos, texts, emails, and Venmo account, requires the phone to be fully encrypted. Ensuring that a disillusioned employee at Apple can't abuse their needed access to the servers that host iMessage to read customer's texts requires that the messages are end-to-end encrypted. Banning encryption is analogous to banning the use of locks and safes, and hoping that, since stealing is a crime, people won't steal.[25]

However, while technologists argue that criminals will always have access to strong end-to-end encryption, there are some benefits to making access to end-to-end encryption difficult or abnormal. In an effort to reduce the degree to which their platform is used to distribute child sexual abuse materials (CSAM), Facebook applies machine learning to all images uploaded to detect even benign child nudity or known CSAM images. End-to-end encryption would prevent this work, and sophisticated criminals who wish to traffic in

[23]Pagliery, Jose. "Terrorists Hide Plans by 'Going Dark'." *CNN Business*, 16 Nov. 2015, https://money.cnn.com/2015/11/16/technology/terrorists-go-dark/index.html.

[24]Goodin, Dan. "US Wants Facebook to Backdoor WhatsApp and Halt Encryption Plans." *Ars Technica*, 3 Oct. 2019, https://arstechnica.com/information-technology/2019/10/ag-barr-is-pushing-facebook-to-backdoor-whatsapp-and-halt-encryption-plans/.

[25]Gallagher, Sean. 'Barr says the US Needs Encryption Backdoors to Prevent "Going Dark." Um, What?' *Ars Technica*, 4 Aug. 2019, https://arstechnica.com/tech-policy/2019/08/post-snowden-tech-became-more-secure-but-is-govt-really-at-risk-of-going-dark/.

CSAM will most likely always have access to the encryption needed to securely transmit these images. However, as part of Facebook's efforts to decrease the effectiveness of their platform as a tool for child predators to meet and exploit children, Facebook also applies machine learning to any text conversation between a child and what seems to be a stranger. They use this to detect whether the conversation appears to be an effort to "groom" the child, and then whether to ban the adult from the platform and/or refer them to law enforcement.[26] Widely available end-to-end encryption would make it impossible for Facebook to scan conversations between parties for problematic behaviour, just as it would prevent them from scanning the conversations for advertisement targeting.[27]

[26]Davis, Antigone. "New Technology to Fight Child Exploitation." *Facebook*, 24 Oct. 2018, https://about.fb.com/news/2018/10/fighting-child-exploitation/.

[27]"Episode 342: Could European Privacy Law Protect American Child Molesters?" The Cyberlaw Podcast. Steptoe and Johnson. 15 Dec. 2020, https://www.steptoe.com/en/news-publications/episode-342-could-european-privacy-law-protect-american-child-molesters.html.

5 Privacy from Megacorporations

Megacorporations control and shape almost all of Americans' interactions with a computer and certainly the internet. Microsoft, Google, and Apple control the most popular operating systems around the world (Windows, Android, and MacOS and iOS, respectively), and Microsoft and Google are perceived as using that power to implement massive and expansive data collection on their users.

In this section, we begin with a series of case studies on privacy violations committed by megacorporations. Some of these actions were illegal, sometimes solely because the company had voluntarily promised not to breach privacy, rather than public policy prohibiting it. Many of these were not illegal. Afterwards, we discuss existing laws, in the US and in other jurisdictions, that attempt to address some of the data practices implicated by these issues.

5.1 The Long History of Tech Privacy Invasions

In this section, we summarize a number of recent invasions of consumer privacy. These are drawn primarily from the last decade, but the history is significantly longer and this is far from a complete list of even the last decade.

Readers who read this section and aren't creeped out or terrified should do their own research until they are.

5.1.1 Windows 10 Telemetry

Historically, Microsoft's Windows gathers so-called telemetry data, or data about how it is being used to send home to Microsoft so they could better understand what parts of their Operating System were being used and what issues users were facing. Up through Windows 8.1, this data collection was Opt-In, requiring users to agree to affirmatively agree to hand over their data. Concerns remained about Microsoft designing their user-interface to encourage users to choose to upload their data, which cast doubts on the authenticity of the user consent. Microsoft, however, laid these concerns about the user consent being poorly informed to rest, by reworking the entire concept of telemetry in Windows 10 to make it far more expansive and far harder to disable.

In Windows 10, Microsoft switched from Opt-In consent to allowing users to Opt-Out of some data collection and not asking for consent for the rest. Users must transmit

telemetry data up to Microsoft, unless they pay for a subscription to Microsoft's corporate version of Windows. In a further transformation of telemetry, Microsoft greatly expanded the scope of data gathered and the purposes which they claim they will use it for. Among the data gathered and reported back to Microsoft by default: the user's location, recordings of all interactions with Cortana and other speech recognition programs, and "diagnostic data". "Diagnostic data" includes what applications you use and for how long, what you do inside the apps, all hardware attached to your device, and data on your typing habits and practice. Microsoft claims that it collects this data for multiple purposes: diagnostics to facilitate improving Windows, tailoring the user experience by recommending Microsoft products, and to facilitate Microsoft's efforts to tailor ads towards your interests.[28]

The last purpose is expansive and sweeping. Microsoft, combining this with the other data they gather about you, uses it to carefully tailor what ads they show you based on the characteristics they derive from studying your browsing habits and all the other data they gather about you. Microsoft uses this data to try and show you better targeted ads, and therefore increase their ad revenue.

All of this behaviour is unambiguously legal in the United States.

5.1.2 Google Location Tracking

Google has been repeatedly accused, by the state of Arizona, the Associated Press, and in various civil suits, of recording user location data even when users affirmatively opted out.[29] The issue here is primarily over the sheer confusion Google's privacy menus entail. Google often changes default values between versions, preventing third parties from maintaining accurate documentation of Google's privacy practices and how to change settings. Google requires users to opt out of data collection in multiple distinct menus and generally does everything it can to confuse users into accepting their surveillance. As of December 2020, litigation to determine whether or not Google's confusing privacy settings are legal is ongoing.[30]

[28]Bright, Peter. "Microsoft Opens up on Windows Telemetry, Tells us Most of What Data it Collects." *Ars Technica*, 5 Apr. 2017, https://arstechnica.com/information-technology/2017/04/microsoft-opens-up-on-windows-telemetry-tells-us-most-of-what-data-it-collects/.

[29]Paresh, Dave. "Google Faces Lawsuit Over Tracking in Apps Even When Users Opted Out." *Reuters*, 14 July 2020, https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit/google-faces-lawsuit-over-tracking-in-apps-even-when-users-opted-out-idUSKCN24F2N4.

[30]Romm, Tony. "Arizona Sues Google over Allegations it Illegally Tracked Android Smartphone Users' Locations." *The Washington Post*, 27 May 2020, https://www.washingtonpost.com/technology/2020/05/27/google-android-privacy-lawsuit/.

Google has also applied this data in a number of ways that distinctly lacked user consent. Notably, in one case they correlated user searches for food poisoning and for various symptoms of food poisoning with the user's location history in order to find which restaurants the user had recently been to. Google then delivered this data to local health officials who conducted inspections of the restaurant and tended to find health code violations.[31] Users had consented only to Google tracking their location history for generic and vaguely described purposes which used live traffic estimation as an example. It was not clear that they would be used to target restaurants with law enforcement actions. Further, concerns about the accuracy of the data raise deep concerns about private companies being able to shape official government behaviour. *This was unambiguously legal.*

5.1.3 Cell Phone Location Tracking by Carriers

In mid-2018, the media reported on a number of small location tracking companies selling location data. Sadly, all of these services had terrible cybersecurity and, according to Brian Krebs, a famed cybersecurity journalist, summarizing Robert Xiao, a then-PhD candidate now-faculty at CMU, "anyone with a modicum of knowledge about how websites work"[32] could look up the location of any cell phone in the United States given just its phone number.[33]

To be clear, every major cell phone company in the United States was selling the real-time location of all of their customers, *including customers who had their Location setting on their phones turned off*, to small third party firms that would then resell that data to paying customers and accidentally leak that data to anyone using the internet. Consumers neither consented to the data collection nor were aware that data collected would be shared publicly.

The accuracy of the data is relatively low by modern location tracking standards, with at best about a mile of precision and based off the Cell Site Location Information; however,

[31]Sadilek, Adam, et al. "Machine-learned Epidemiology: Real-time Detection of Foodborne Illness at Scale." *npj Digital Med*, vol. 1, no. 36, 6 Nov. 2018, https://doi.org/10.1038/s41746-018-0045-1.

[32]Krebs, Brian. "Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site." *Krebs on Security*, 17 May 2018, https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/.

[33]Gallagher, Sean. "Company Used by Police, Prisons to Find any Mobile Device Breached (Again)." *Ars Technica*, 16 May 2018, https://arstechnica.com/information-technology/2018/05/company-used-by-police-prisons-to-find-any-mobile-device-breached-again/.

the Supreme Court did hold in *Carpenter v. US* that this data is accurate enough for law enforcement to need a warrant if they want to compel the disclosure of the data, as it has significant applications in violating someone's privacy.

After *Carpenter v. US*, law enforcement lost access to this location data without a warrant; however, these data brokers provide a way out of the warrant requirement. Buying the location data from industry does not require a warrant and can be done much more broadly then it was possible to do previously. This concerning hole in American law could be closed by either making some data, such as location data, protected, so third parties can't willingly disclose or sell it, or by prohibiting law enforcement from buying what they can't obtain through legal channels, though that raises other issues.

The FCC concluded that selling this location data without consent was illegal two years after the violations came to light; however, the proposed penalties were quite small compared to the revenues of the companies in question and further litigation can only decrease the size of the penalties.[34]

This scandal highlights the lack of effective enforcement of existing privacy laws.

5.1.4 Facebook Research Study on Emotions

In 2014, Facebook published an academic study that showed that users who are shown more negative content feel more negative emotions and those shown more positive content feel more positive emotions. The methods of the study: randomly selecting users and changing what they observed and then measuring mood changes based on changes in posting patterns. This launched a backlash against Facebook, with many users creeped out at the idea that they may have been manipulated by Facebook for a research study. The only user consent obtained was the standard consent to access the site.[35] No users were notified that they had participated in the study. Some—including an op-ed in *Ars Technica*,[36] reporting in *The Washington Post*,[37] and Randall Munroe in the comic reproduced in

[34]Brodkin, Jon. "FCC Issues Wrist-slap Fines to Carriers that Sold Your Phone-location Data." *Ars Technica*, 28 Feb. 2020, https://arstechnica.com/tech-policy/2020/02/fcc-issues-wrist-slap-fines-to-carriers-that-sold-your-phone-location-data/.

[35]Kramer, Adam, James E. Guillory, and Jeffrey T. Hancock. "Experimental Evidence of Massive-scale Emotional Contagion through Social Networks." *Proceedings of the National Academy of Sciences*, vol. 111, no. 24, 17 June 2014, pp. 8788–8790. https://doi.org/10.1073/pnas.1320040111.

[36]Johnston, Casey. "Facebook's Emotional Experiments on Users aren't All Bad." *Ars Technica*, 30 June 2014, https://arstechnica.com/information-technology/2014/06/facebooks-emotional-experiments-on-users-arent-all-bad/.

[37]Dewey, Caitlin. "9 Answers about Facebook's Creepy Emotional-manipulation Experiment." *The Washigton Post*, 1 July 2014, https://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-

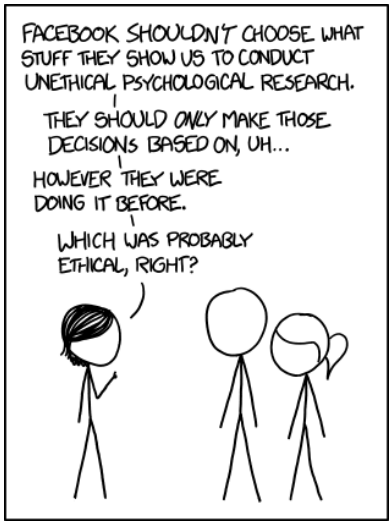


Figure 2: The alt text is "I mean, it's not like we could just demand to see the code that's governing our lives. What right do we have to poke around in Facebook's private affairs like that?"[a]

[a]Munroe, Randall. "Research Ethics." *xkcd*, https://xkcd.com/1390.

Figure 2—defended the study, not necessarily as ethical, but as well within the bounds of normal so-called "A/B testing" conducted everyday on the platforms and which are often focused on increasing engagement.

The ethics questions raised here may fall outside the scope of this session of the Senate. It reaches deep into how social media works in this country and the general approach to software development where testing new features on live users is considered standard and appropriate.

5.1.5 The Cambridge Analytica Scandal

Most user's interactions with social media sites like Facebook or TikTok reveals an incredible volume of information about them. To quote the 2013 paper that helped pioneer the technology at the heart of the Cambridge Analytica scandal,

> We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and

answers-about-facebooks-creepy-emotional-manipulation-experiment/.

> political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. …
>
> People may choose not to reveal certain pieces of information about their lives, such as their sexual orientation or age, and yet this information might be predicted in a statistical sense from other aspects of their lives that they do reveal. …
>
> This study demonstrates the degree to which relatively basic digital records of human behavior can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private.[38]

An accurate profile of a person's internet browsing or social media use is sufficient to, with high accuracy, infer private information about the person. The 2013 paper by Kosinski, Stillwell, and Graepel demonstrated its feasibility. A year later, a data analytics firm, Cambridge Analytica, began to provide support for another academic study. But Cambridge Analytrica did not just gather data on the subjects of its study. It bought data from an academic-turned-entrepreneur who had made a fairly popular app that sucked up as much data as it could. The academic-turned-entrepreneur could not legally sell the data per his agreement to access the data from Facebook, but he defends the morality of his actions by highlighting Facebook's rare enforcement. This allowed Cambridge Analytica to grow the number of Americans it could create profiles on to an ever-increasing size, eventually gathering data on tens of millions of Facebook users, many of whom had not consented to their data being collected.

Cambridge Analytica then sold access to this dataset to political campaigns who would use the data to micro-target ads towards individual Americans who never consented to their data being used for micro-targeting political ads to them. Cambridge Analytica's most high-profile customers included the successful 2016 American Presidential candidate and the unsuccessful 2016 Presidential Repubican Primary campaign of the Junior Senator from Texas.

Many of the academics involved in the original research and in the data ending up in Cambridge Analytica's hands, place the blame for the unethical use of consumer data

[38]Kosinski, Michael, et al. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." Proceedings of the National Academy of Sciences, vol. 110, no. 15, 9 Apr. 2013, pp. 5802–5805, https://doi.org/10.1073/pnas.1218772110.

firmly on Facebook.[39] Cambridge Analytica could have created its own viral app to suck up data from everyone who used the app and all of their Facebook friends and created the same dataset without any violations of Facebook's Terms of Service. Facebook exposed huge amounts of consumer data to third parties and, in doing so, allowed for the data to be put to potentially unethical uses.[40]

5.1.6 AT&T Monitoring User Traffic

AT&T is an internet service provider (ISP), *i.e.* they provide the physical connection between a customer's home and the internet as a whole. All internet traffic from the customer's home goes through AT&T's computers and servers. In much of the country, Americans have access to only one ISP and suffer under an effective monopoly.

In 2013, AT&T announced a new program for the subscribers to its fastest internet offerings in which AT&T would track "the webpages you visit, the time you spend on each, the links or ads you see and follow, and the search terms you enter"[41]. AT&T would then use this data to better target the advertisements you see on the internet, receive to your email inbox, and receive in your physical mailbox. Keep in mind that AT&T is watching all the traffic passing from a house, without any way to differentiate between different users or devices. Using "Incognito Mode" has no impact on this surveillance. A teenaged child accessing the Trevor Project's emergency support line for LGBTQ+ youth would be recorded by AT&T who might start showing LGBTQ+ targeted advertising to the entire family. AT&T did provide a method to opt-out of this surveillance: pay an additional $744 per year for internet.[42]

AT&T ended this program for unknown reasons in 2016.[43] One notable theory for

[39]Lapowsky, Issie. "The Man Who Saw the Dangers of Cambridge Analytica Years Ago." *Wired*, 19 June 2018, https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica/.

[40]Wong, Julia Carrie. "The Cambridge Analytica Scandal Changed the World – but it didn't Change Facebook." *The Guardian*, 18 Mar. 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

[41]Quoted in Brodkin, Jon. "AT&T's Plan to Watch your Web Browsing—and what you can do about it." *Ars Technica*, 27 Mar. 2015, https://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/.

[42]Brodkin, Jon. "AT&T Offers Gigabit Internet Discount in Exchange for your Web History." *Ars Technica*, 11 Dec. 2013, https://arstechnica.com/information-technology/2013/12/att-offers-gigabit-internet-discount-in-exchange-for-your-web-history/.

[43]Brodkin, Jon. "AT&T to End Targeted Ads Program, Give All Users Lowest Available Price." *Ars Technica*, 30 Sept. 2016, https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.

why AT&T chose to end the program was due to the FCC implementing stricter rules on ISP surveillance of consumers; however, those rules were repealed in 2017 by the Republican-controlled Congress and newly elected Republican President.[44]

This is entirely legal. Further, even if AT&T didn't run their own ad network, they could legally sell the data to the other ad networks. Or just sell the browsing data to any other company that wants to buy the data for any purpose.

5.1.7 Apple Employees Listening to Siri

It was revealed in July of 2019 that Apple had been storing and reviewing "a small portion of Siri requests" to be used to improve the virtual assistant's ability to understand users. This practice came to light when a whistleblower who personally listened to the short clips while working for a firm contracted by Apple came forward. Siri, and therefore these short recordings, were often activated accidentally and were likely to record confidential, sensitive and otherwise private information. This included doctor and patient conversations and what the whistleblower believed was criminal activity.[45]

Following the release of the article, Apple put out a statement in which it promised to temporarily halt the review program until such a time that improvements could be made. The first two of its promised changes were to allow users to opt-out of the data collection process and that by default only transcripts of the data would be collected and stored. In response to the outrage over the use of contractors to review their data, Apple also promised that going forward only Apple employees would review the stored audio samples and transcripts. Regardless of the changes made, consumer's private data is still being listened to by other private citizens, even if they do work for Apple. While the company holds that no personally identifiable data is stored alongside the recordings, the whistleblower claimed that the information audible during the recordings often made it easy to identify the parties involved.[46]

Apple's practices may have been illegal, but only because they breached the privacy

[44]Brodkin, Jon. "President Trump Delivers Final Blow to Web Browsing Privacy Rules." *Ars Technica*, 3 Apr. 2017, https://arstechnica.com/tech-policy/2017/04/trumps-signature-makes-it-official-isp-privacy-rules-are-dead/.

[45]Hern, Alex. "Apple Contractors 'Regularly Hear Confidential Details' on Siri Recordings." *The Guardian*, 26 July 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

[46]Hern, Alex. "Apple Apologises for Allowing Workers to Listen to Siri Recordings." *The Guardian*, 29 Aug. 2019, https://www.theguardian.com/technology/2019/aug/29/apple-apologises-listen-siri-recordings.

policy Apple requires users to agree to in order to use Siri. Apple could have easily reserved the right to tap users at will, and to sell any data gleaned.

5.1.8 State Governments Selling DMV Records

The California DMV, along with many other state's DMVs in the country, sell driver's personal information to companies seeking to buy it. The California DMV in a single year made around $50 million from the selling of personal information on registered drivers.[47] Their customers included a number of private investigator firms that market themselves as investigating infidelity and offering surveillance. There has also been a history of abuse of data access according to other states' DMV, but details have not been forthcoming.[48]

Many purchasers have some legitimate uses of driving data such as auto insurance providers, car manufacturers trying to understand what vehicles are in use, and other automotive-related customers. The primary policy concern here is about citizens, forced to hand over personal information in order to drive or own cars, are forced to accept that data being resold by the government for revenue generation.

5.2 Existing Laws

5.2.1 Children's Online Privacy Protection Act

In response to concerns in the 1990s that websites were collecting personal information from minors, Congress passed the Children's Online Privacy Protection Act, which went into effect on April 21, 2000. The legislation gave the FTC the authority to penalize US-based firms that collected information from minors under the age of 13 without their parent's verifiable consent. The FTC has detailed guidance regarding how online services should obtain parental consent, but implementing them is expensive, since many approved forms of parental consent require the attention of a real staff member or specialized software.[49]

[47] Cox, Joseph. "California DMV Is Selling Drivers' Data to Private Investigators." *Vice Motherboard*, 18 Aug. 2020, https://www.vice.com/en_us/article/dyzeza/california-dmv-data-private-investigators/.

[48] Cox, Joseph. "DMVs Are Selling Your Data to Private Investigators." *Vice Motherboard*, 6 Sep. 2019, https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars.

[49] "Children's Online Privacy Protection Act (COPPA)." *Electronic Privacy Information Center*, https://epic.org/privacy/kids/.

In order to avoid violating COPPA, many websites and online services simply require all users be 13 years of age or older. This practice is criticized for encouraging age fraud as many sites have easily circumventable age verification systems. Some services have found other ways to treat those 12 and under.

In 2019, Google's YouTube implemented a "For Kids" tag to put on videos after the FTC ruled that the service violated COPPA. This practice saw backlash from many of the site's content creators as videos with the "For Kids" tag use contextually targeted ads—instead of the more profitable customer-specific ads typically used online—and do not allow creators to include end-screens that increase viewer retention. Further, YouTube mandated that creators mark their own videos as made for kids, but YouTube failed to explicitly define what qualifications a video must meet to be "For Kids". As the FTC asserted that it was capable of directly suing individual content creators that violated its regulations, content creators whose productions could be seen as kid-friendly, but who did not target children as their primary audience, were forced to balance the risk of facing possibly expensive legal consequences against the certainty of losing large parts of their incomes to the restrictions placed on "For Kids" videos. The challenges creators faced were largely created by the binary system that videos were sorted into. YouTube could have avoided these issues by implementing a "mixed audience" tag and then had YouTube's ad system treat viewers of "mixed audience" content differently based on their age. This system would require an FTC-compliant age verification system. YouTube must have concluded that designing and implementing such an age-verification system would be too costly and not profitable, and chose to leave the burden on content creators to police themselves or face large penalties. Separately, the FTC was criticized for the settlement which led to the creation of "For Kids" for only fining YouTube $170 million. The critics, who include one of the FTC commissioners, argue the fine is "a rounding error" in YouTube's average annual income of $20 billion.[50]

As with many internet regulations, Congress's goal in COPPA is sound, as protecting childrens' privacy is functionally universally supported among Americans; however, the implementation has proven to be difficult and expensive, encouraging companies to try to work around the legislation. It is imperative to recognize the complications of implementing acts like COPPA. There are far-reaching consequences for the solutions to problems as legitimate as child privacy—though the intentions are sincere, the effectiveness

[50]Jennings, Rebecca. "The Golden Age of Kids' Youtube is Over. Good." *Vox*, 20 Dec. 2019, https://www.vox.com/the-goods/2019/12/20/21025139/youtube-kids-coppa-law-ftc-2020.

of a policy should not and cannot be solely measured by how strict it is. The harms caused by the implementations of the policy must be seriously considered, especially the risk that they hurt the very people it was intended to protect.

5.2.2 The Global Data Protection Regulation of the European Union

In an attempt to assert protection for European consumers' personal data, the EU passed the Global Data Protection Regulation, a law which outlines specific requirements that any firms handling EU citizens' data must comply with. The 99 articles of the GDPR touch on a wide variety of topics but this committee will focus on the following four: the minimisation of data collected, the roles and responsibilities of data controllers and processors, the rights that consumers have with respect to their data, and the penalties for non compliant firms.

Data minimisation and purpose limitation are guiding principles of the GDPR. Conceptually, they're very similar; both restrict the data collected from consumers and the collected data used to the smallest possible quantities. Data minimisation applies to the storage of consumer data, and requires that firms handling the data must ensure they have only the data needed to properly execute their services.[51] Purpose limitation means that all collected data must have an explicit connection to the sought service, and that the collected data should not be processed for any purpose besides the original.

According to the GDPR, there are two parties that assume responsibility for how a consumer's data is handled, controllers and processors. Controllers are defined as the legally identifiable person(s) or body who decides the "purposes and means of processing" a consumer's personal data.[52] Processors are defined as the legally identifiable person(s) or body that is responsible for implementing the methods of using consumer data that controllers have decided upon.[53]

Controllers are required to ensure that personal data is processed and protected in ways that abide by the regulation's complete text, and they should take into account the context of technological advancements and costs. The GDPR also mandates that should the controller become aware of a data breach, within 72 hours of learning of the breach

[51]Marr, Bernard. "Why data Minimization Is An Important Concept In The Age of Big Data." *Forbes*, 16 Mar. 2016, https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#653f6e2b1da4.

[52]Chapter 1, Article 4. *General Data Protection Regulation (GDPR)*. OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

[53]*ibid*.

they must notify EU authorities.[54]

Processors are required to act in accordance with their controller's decisions for data processing and have little to no autonomy.[55]

Both parties must keep detailed records including the names of involved controllers and processors, the methods in which processing is carried out, and other information relating to the handling of consumer's personal data.

Chapter 3 of the GDPR outlines the rights of the consumers being surveilled. Consumers are guaranteed the right to transparency of data collection and access to the means of exercising their other rights. Controllers must inform consumers of their intent to collect personal information and provide means of contacting those responsible for managing data collection and processing. In cases when a secondary controller is provided a consumer's personal data for any reason, the initial controller of the consumer's data must provide the contact information of the secondary data controller, so that the consumer can exercise their rights.Data controllers must provide information relating to the purpose of the processing in response to consumer requests. Consumers have the right to correct outdated data that has been collected, to complete incomplete sets of data, or to request erasure of their personal data. Controllers are required to comply. Additionally, consumers have the right to prohibit the processing of their data without erasure. Data portability rights mean that a consumer's data must be available to them in a format that is easily readable and can be transported to another controller without undue hindrance. Finally, consumers may object to the processing of their data and force the controller to halt until they can prove a legitimate legal basis to continue. Article 23, however, provides for several contexts in which the consumers' abovementioned rights may be abridged or restricted.[56]

Firms that are found noncompliant with the GDPR can face heavy penalties. Depending on the violated article and severity of noncompliance, an individual case can incur fines ranging from 2%–4% of the company's "total worldwide annual turnover of the preceding financial year".[57] These fines are most often to be measured in ten of millions of dollars, but can be much larger depending on the size of the firm. Should Apple be

[54]Chapter 4, Article 24. *General Data Protection Regulation (GDPR)*. OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
[55]Chapter 4, Article 28. *General Data Protection Regulation (GDPR)*. OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
[56]Chapter 2. *General Data Protection Regulation (GDPR)*. OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
[57]Chapter 8, Article 83. *General Data Protection Regulation (GDPR)*. OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

found in violation, they could face fines up to $2.2 billion in 2020.[58]

As the primary data privacy regulations for the European Union, one of the largest economies in the world, the GDPR exerts large scale influence on worldwide data privacy policy and practices. The GDPR only applies inside the EU, allowing it to heavily affect the practices of international firms who are forced to build the needed infrastructure for compliance.

The GDPR decreases consumers' digital footprint. Data minimization finds its main value in data security. While there may be an ethical argument to be made for data minimization in the context of limiting the knowledge firms have of their consumers, it primarily serves to protect consumers from parties with ill-intentions. When a firm has less information on record for any given consumer, there is less information for unauthorized parties to take advantage of in the case of a breach.

In many ways the regulations outlined in the GDPR serve to realign the information interchanged in online transactions between consumers and services with the information interchanged during in-person transactions.

Think briefly about how much information a consumer gives a flower shop when purchasing a bouquet in-person. By choosing not to share any personal information, they can make themself functionally untraceable to the shop owner with the exception of their appearance and implying that they may live nearby.

When attempting to purchase that same bouquet online there is a much larger quantity of information that they provide, either unintentionally or without alternative. Visiting the shop online marks them as a potential target for flower advertisements in the future. Often they will need to create an account to complete their purchase, and—therefore—provide their contact information. They also need to provide a shipping address, exposing their exact geographic location.

The GDPR's regulations call for data minimization and data transparency so that consumers can know what information they are sharing and its relevance to the transaction at hand. Such regulations make steps toward bestowing a sense of anonymity and privacy to the internet for EU consumers.

[58]"Apple's Net Income in the Company's Fiscal Years from 2005 to 2019." *Statista*, Oct. 2019, https://www.statista.com/statistics/267728/apples-net-income-since-2005/.

5.2.3 California Consumer Privacy Act

Simply providing consumers with the rights to protect their privacy and personal information means little if they aren't aware of—and therefore cannot exercise—those rights. The California Consumer Privacy Act mandates that businesses that collect their consumer's personal information must notify consumers of this collection and of their right to opt out. It requires notices that must be presented to consumers before or as data collection begins. It further mandates that the option to opt out of data collection must be readily available to consumers, and that the opt-out be described in clear language free of technical or legal jargon. In some ways, the CCPA is modeled off the GDPR and was certainly inspired by the successes of the EU's privacy regulation scheme.[59]

While there are definite similarities between both sets of regulations, there is a clear distinction to be made. Importantly there is the difference in scope, the CCPA is limited in applicability to for-profit businesses that meet at least one of the following thresholds: makes 50% of its revenue from selling California resident's personal data, has a gross annual revenue of at least $25 million, or "buy[s], receive[s], or sell[s] the personal information of 50,000 or more California residents, households, or devices". Additionally, the CCPA ensures consumers the right to opt-out of data collection. The GDPR requires companies obtain consent from EU-based users, *i.e.* requires consumers opt-in to data collection.[60]

Some of the other differences between the two laws are easier to miss. Both the GDPR and CCPA acknowledge that in certain cases, data about a consumer should not be given the same protections as consumer data. In the GDPR, these instances are not directly or specifically mentioned and are left open for interpretation by Courts and regulators. Whereas, in the CCPA the exceptions to the usual consumer data protections are specifically named, for example, publicly-available information is not protected by the CCPA.[61]

Another distinction is that the CCPA does not explicitly require data-handling firms to meet reasonable security measures, and instead allows consumers adversely affected by a breach to file a civil lawsuit against firms that failed to meet expectations of reasonable security measures.[62]

[59]Section 1798.185.6. "California Consumer Privacy Act (CCPA)." Office of the Attorney General, https://oag.ca.gov/privacy/ccpa.
[60]Section 1798.140. "California Consumer Privacy Act (CCPA)." Office of the Attorney General, https://oag.ca.gov/privacy/ccpa.
[61]*ibid*.
[62]Section 1798.150. "California Consumer Privacy Act (CCPA)." Office of the Attorney General, https:

In general, the CCPA is quite specific in how regulations can be applied and who they apply to. There is very little space to misunderstand the intentions of each piece of the CCPA. This specificity makes both enforcement and compliance simpler and cheaper for all parties involved.

The difference between the GDPR's generality and the CCPA's specificity represents two possible pathways for data privacy regulation. The specific outlining and referencing of costs, types of data, and expected levels of protection in the CCPA presents a more easily complied with law, with clear objective rules for firms to follow and straightforward enforcement. The broad strokes approach of the GDPR leaves much more room for interpretation of what is compliant and noncompliant.

5.2.4 California Privacy Rights Act

In November 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA). Taking effect on January 1, 2023, the CPRA is an expansion of the CCPA, which went into effect on January 1, 2020.

The new regulations of the CPRA increase consumer rights, establish new protections for personal data, and expand penalties for mishandling personal data. The CPRA introduces new rights enforceable against corporations for the consumer's sensitive personal information, which includes Social Security Numbers, ethnicity, religion, and precise geolocation data. The CPRA's enforcement structure exempts more small businesses than the CCPA, but increases the size of monetary damages and removes the CCPA's warning period to corporations found in violation. Further, the CPRA establishes the California Privacy Protection Agency (CPPA) which has jurisdiction over violations of the CCPA and CPRA. The agency has a five member governing board, who will oversee investigations into possible CCPA and CPRA violations, provide guidance for confused consumers and businesses, and develop regulations. Previously enforcement was handled by the California Department of Justice.[63]

//oag.ca.gov/privacy/ccpa.

[63]Cole, Cynthia, Matthew Baker, and Katherine Burgess. "Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now." *Bloomberg Law*, 16 Nov. 2020, https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now.

6 Conclusion

In this section, the Dias will aim to highlight the key takeaways from the discussions of technology above. We aim to focus on the most counter-intuitive components and the issues with the naive solutions to these challenges. Senators are expected to design solutions that clearly avoid these fatal flaws.

6.1 Court-Controlled/Court-Aware Cryptography

Throughout debates about encryption it is incredibly tempting to declare "we should have courts control a master encryption key" so it can only be used under a court's permission. Either the system would have no mathematically verifiable security guarantees, or the Court would be required to have a secret file that it can still access when needed. These secret files would be stunningly valuable, and therefore, there is little to no chance of actually preserving their security considering that even the NSA has failed to keep its exploit database secret in the past.[64]

Any scheme that trusts Courts to maintain a secret must have a clear plan for what to do when the secret is obtained by criminals and the plan must ensure that it doesn't undermine security.

Former-FBI Director James Comey repeatedly asked Congress to mandate that all encrypted systems have a "golden key" which could allow the FBI to circumvent the encryption if it was legally allowed to.[65] No such "golden key" can exist without either sacrificing the mathematical guarantees on security given by modern cryptography or a Court holding a secret file. Any proposal which includes a call for a "golden key" but doesn't address this issue is fundamentally unserious. If Senators wish to make such a proposal, the Dias expects them to either explicitly acknowledge the economic and security cost of their proposal or to present a clear explanation of why and how their scheme will remain secure should the secret files become public.

[64]" 'NSA Malware' Released by Shadow Brokers Hacker Group." *BBC*, 10 Apr. 2017, https://www.bbc.co.uk/news/technology-39553241.

[65]Gallagher, Sean. "What the Government Should've Learned about Backdoors from the Clipper Chip." *Ars Technica*, 14 Dec. 2015, https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

6.2 International Precedent

If the US requires corporations to do something, every other country can. If the US adopts a law mandating disclosure of data from anyone world over to the government, every other country will feel emboldened to make the same demands. For countries which are major markets for tech companies, such as China, Russia, and much of the EU, the companies will be forced to comply. American protections, such as "get a warrant", will likely not be meaningfully emulated by countries such as China and Russia with little history of rights for criminal defendants.

If the US mandates James Comey's "golden key" be added to all encryption systems allowing the government to bypass any technological attempt to secure data, other countries will follow suit, and soon secure communication between US spies and their handlers will be forced to either be accessible to the state the spy is operating in or to be criminally secure speech, which is just as likely to attract the attention of authorities.

6.3 Disparate Impacts of Compliance

Compliance with stringent regulations can be expensive; this cost is a lot easier to swallow for larger corporations that have functional revenue streams that allow them to invest in compliance. Smaller players in the marketplace, who may not yet be producing money, are forced to not invest in features in order to comply with regulations.

The simplest solution to this problem is normally a graduated ramp up of obligations for increasingly large corporations or products. Caution is warranted with this approach though, as products can become rapidly popular. Overnight changes to which regulatory regime is binding, based on an overnight surge in either users or revenue, can destroy a new entry in the marketplace as fast as anything else.

6.4 Further Readings[66]

To better understand the underlying technology that underpins modern debates on data privacy, it may be beneficial to read a detailed introduction to how computers and computer

[66]Some of these readings come from sources who have their own policy agendas or backgrounds, and interpret the facts to be most convenient for their narrative. The Dias, personally, disagrees with some of these ideas. Senators are encouraged to read these sources critically and not as direct policy recommendations from the Dias. Although we do expect well-researched debate, the Dias does not view this section as necessary reading and considers it to be strictly supplementary to the rest of this background guide.

networks work written for a law student audience. The Dias recommends Chapter 1 of *Internet Law: Cases and Problems* by Professor James Grimmelmann. The book is available at http://internetcasebook.com/ for whatever price you feel is ethical.

For a more detailed look at existing laws and the constitutional issues surrounding digital privacy, the Dias recommends Chapter 4 of Grimmelmann's *Internet Law: Cases and Problems*. For an interesting policy proposal (that could be established by statute rather then by the judiciary as the author suggests) and a good read on the Stored Communications Act's interpretation and application, see Professor Rebecca Wexler's article in the *Harvard Law Review* titled "Privacy As Privilege: The Stored Communications Act and Internet Evidence" and available for free on SSRN. For Professor Orin Kerr's guide to understanding the Stored Communication Act (and for his suggestions on how to amend it), see "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it" published in the *George Washington Law Review* and available on SSRN. On FISA, the Council on Foreign Relations recently published a very approachable introduction to the controversies surrounding FISA by Glenn S. Gerstell, former general counsel of the National Security Agency. They are available as "Making Sense of the Debate over FISA (Part One)" and "FISA's Current Controversies and Room for Improvement (Part Two)".

For a separate analysis of the GDPR and how firms prepare themselves to comply, please see the "Guide to the General Data Protection Regulation (GDPR)" by the Information Commissioner's Office of the UK. For a look into the feasibility of compliance under the GDPR, see "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions" by Eugenia Politui, Efthimios Alepis, and Constantionos Patsakis. For a more detailed discussion of the differing dynamics between the GDPR and CCPA, see Catherine Barrertt's "Are The EU GDPR And The California CCPA Becoming The De Facto Global Standards For Data Privacy And Protection?".

6.5 Questions to Consider

6.5.1 Privacy from Government

- How should law enforcement be able to access foreign data about US persons accessible from US computer systems? Foreign data about foreign persons accessible from US computer systems? Is the CLOUD Act sufficient? Should we adopt a data localization regime similar to Russia? How would such a data localization regime

be enforced without Russian-style banning of entire websites?

- How should the Stored Communications Act be updated to reflect the changes in the use of email? Should the intent of the 1986 Congress to protect emails from warrantless access be restored? Should rights be curtailed?
- Should FISA be reformed? If so, how?
- Should a Court be able to require an American corporation to retroactively weaken the security of its products to assist law enforcement? What about non-American corporations?
- Should compelled password disclosure be curtailed? Prohibited? How does Congress protect people who genuinely forgot a password? How does Congress ensure law enforcement has access to the incentives they need to ensure citizens comply with orders?
- Should Congress intervene in the "Going Dark" debate? Mandate backdoors in encryption? Criminalize secure encryption? Prefer the status quo which protects US consumers from hackers?

6.5.2 Privacy from Megacorporations

- How should Congress intervene in the practices of tech companies? Should data collection be restricted? Should there be limits in how collected data is used? Should there be restrictions on sharing data with other parties?
- Should some data be considered particularly sensitive and subject to greater protection? Should law enforcement be able to buy location data from cell phone companies that they can't lawfully subpoena?
- Should some types of data be considered less sensitive and subject to lesser protections?
- Should restrictions be placed on government bodies selling consumer data?
- Should certain data be illegal to process by humans? Should certain data be illegal to process exclusively by computers?
- Should children have greater protections?
- How should specifics of the law be determined? Will Congress write detailed and all-encompassing legislation? Will power be delegated to an agency? Will meaning form as part of common law litigation?
- How will the law be enforced? Will consumers have a right of action? Will there be

an independent federal agency tasked with civil enforcement? Will the Department of Justice be in charge of criminally prosecuting violations of the law?

- Who is liable and what are appropriate punishments for violations of the law? Can top executives receive jail time for violations? Should punishments be determined in absolute dollar amounts? As a percentage of gross domestic income? As a percentage of gross global income?

A United States Senate Rules

A.1 The Filibuster

Out of respect for Senate traditions, the Dias will allow filibusters, subject to some mild constraints.[67] A Senator may only filibuster the Speaker's List and in Voting Bloc. The Senator must inform the Dias at the beginning of their speech of their intent to filibuster and present to the Dias an original solution of at least one currently unsolved Millennium Prize problem.[68] Throughout a filibuster, the Senator must speak exclusively in quotes of at least 20 words from the writings of Dr. Seuss. The Senator must be prepared to present the Dias with written citations for each quote. The Senator may not use a pen or other writing instrument. The Senator must not use the same quote twice.

A.2 Cloture

As there is always the risk that a Senator will solve a Millenium Prize problem—which would surely be a major breakthrough in theoretical mathematics—and result in a filibuster, we will modify Voting Bloc to better reflect Senate traditions. Voting Bloc cannot be

[67] "Mild constraints", in this context, means nearly impossible to fulfill.

[68] Preferably, this requirement is fulfilled with a constructive proof of $\mathcal{P} = \mathcal{NP}$ or of $\exists\, x \in \mathbb{C} : \Re\{x\} \neq \frac{1}{2} \wedge x \notin -2\mathbb{Z}^+ \wedge \zeta(x) = 0$. Senators are expected to donate the prize money to a charity of the Dias's choice.

entered with a predetermined number of speeches. Instead, before each round of for and against speeches, any Senator can motion for cloture to end the debate on the Bill or amendment in question. For such a motion to pass, 60% of the number of Senators who have attended that session must vote in favor. If cloture fails, only a Senator who previously did not vote in favor of cloture may motion for cloture. Any Senator can motion to table a Bill, which requires a simple majority.

If the Senate amends its agenda to include judicial nominations,[69] cloture will only require a majority of those not abstaining to close debate on a given nomination.

A.3 Taxes

While the Dias does not anticipate tax policy being pertinent to this debate, we understand that it may be useful or critical to levy taxes against corporations to help shape their behavior. Accordingly, in keeping with Senate tradition and in compliance with Article 1, Section 7, Clause 1 of the US Constitution, the Dias will allow this Senate to fully replace the text of a bill on taxes that originated in the House. In our scenario, the House passed HR243 "To amend the Internal Revenue Code of 1986 to tax the capital gains of United States Senators at 200%". This bill is the most ripe target for this traditional cannibalization, as it has received almost no support in the upper chamber.

A.4 Other Strange Parliamentary Quirks of the US Senate

If you are a particular fan of any other obscure Senate rules or practice, please email us at senate@ucbmun.org. We may hand down additional rules at the beginning of Friday.

[69] The Dias will be deeply concerned about what we did wrong.