Third World Network Preliminary Note:

Electronic authentication: some implications[a]

[a] By Sanya Reid Smith, Third World Network, sanya@twnetwork.org, partially updated in August 2018. With thanks to Richard Hill for his contributions, any remaining errors are Sanya's.

Executive summary

This preliminary note looks at the implications of ecommerce proposals on electronic authentication (eauthentication) in the Regional Comprehensive Economic Partnership (RCEP), Trans-Pacific Partnership (TPP), the World Trade Organization (WTO) and European Union (EU) free trade agreements (FTAs) which require governments to leave it to the private sector to set the authentication methods (that is, the security standards) of electronic transactions (except for perhaps one category of transactions). This note:

- Gives examples of cybersecurity breaches due to insufficient security standards in electronic transactions
- highlights that systemic market failure due to externalities and information asymmetries make such cybersecurity breaches likely to recur without regulation. (As the Internet Society notes about market failures, 'Often government intervention is used to address the failure'). This government intervention/regulation is prohibited/restricted by these ecommerce proposals.
- gives some examples of developing and developed country governments (including subnational governments) setting certain standards for authentication methods for electronic transactions and why they do so (eg consumer protection and privacy), including because leaving it to the private sector to choose their standards had been problematic,
- provides an example of what happened when it was left to the private sector to decide its own standards:
    - expensive and difficult-to-comply–with-standards were set by the dominant companies
    - these standards were insufficiently secure
- notes how the problems caused by this ecommerce proposal can be exacerbated by other ecommerce proposals (or those in other FTA chapters such as services)
- highlights the likely difficulty in using the usual exceptions in trade agreements for privacy, health, prudential reasons etc.

Introduction

Cybersecurity

The Internet Society noted in their 2016 report:[1]

- 'data breaches continue to increase in number, size, and cost' (see Chapter 2 for details[b] which includes a common cybersecurity saying: 'There are two types of companies – those who have been hacked, and those who don't know they have been hacked' and that even cybersecurity companies themselves have been hacked[2]). According to one study, 93% of data breaches could have been avoided based on existing tools, this leaves 7% (eg zero day exploits[c]) which cannot be protected against, so the data at risk must be encrypted so that it cannot be read if hacked.

[b] Although since many countries do not require reporting of breaches, these are underestimates.
[c] These are security vulnerabilities 'that are unknown to the software developer until exposed (giving 'zero days' to fix the vulnerability).'

    - Identity theft is the most common and bank account/credit card details are the second-most frequent breaches.
- The cost of data breaches (which is an underestimate because many countries still do not require data breaches to be reported and the costs to society and the user etc are often not included, see below) were estimated in 2015 to be 'around USD 500 billion, and would quadruple to USD 2.1 trillion by 2019, representing 2.2% of global GDP'

Furthermore, there are widely recognised market failures in cybersecurity. Eg:

- a 2018 US government report noted that 'Market incentives are misaligned. Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.'[3]
- The European Union Agency for Network and Information Security set up by the EU noted in 2016 that 'we are seeing a market failure for cybersecurity and privacy: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy.'[4]

In addition, the Internet Society's 2016 report includes:[5]

- Given the frequency of large data breaches (eg Target had 40 million customers' credit card numbers stolen and put on sale online'), 'The question remains why, given the cost of breaches, more is not done by organisations to address the preventable ones, and to lower the cost and impact of foreseeable ones?' The answer is that:
    - 'There is a market failure that governs investment in cybersecurity. First, data breaches have externalities; costs that are not accounted for by organisations. Second, even where investments are made, as a result of asymmetric information, it is difficult for organisations to convey the resulting level of cybersecurity to the rest of the ecosystem. . . [Ie] The cost of a breach is not entirely borne by the organisation breached, and the benefit of offering better data security is not high enough. . . As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.' Furthermore, 'In countries where disclosure is not even required, the externalities are yet greater, as the companies may not even bear any reputational cost from the breach, further lowering the incentive to invest in cybersecurity.'
    - It explains **externalities** as: 'The breached organisation does not bear all of the costs of the breach – the cost borne by others is an externality that does not necessarily factor into its decisions on how to protect against data breaches.' Eg the hacked organisations 'often do not bear all the financial cost imposed on other related organisations by the breach, and they do not bear all the cost imposed on users. In economic terms these unaccounted for costs are externalities. . .
        - For instance, when Target stores were breached for credit card data, the financial institutions bore the cost of replacing the credit cards, and followed with lawsuits to recover losses from Target. Indeed, Target itself was breached through a connected contractor, whose defences were weaker but it may not have borne any of the direct cost of the breach. Even Target customers, whose credit card details were the target of the breach, had to sue for compensation, finally reaching a legal settlement'.
        - Costs to the user include 'user liability for fraud, time spent on trying to be compensated for fraud and restore their identity and credit, not to mention the non-financial cost in terms of anxiety and uncertainty.' Eg 'One such study showed a significant proportion of victims of stolen US social security numbers were the subject of identity theft. Each incident resulted in USD 3,300 in losses along with 20 hours of time and USD 770 spent on lawyers. It is not clear if these costs were covered in the aftermath of that breach – in general though, users have to fight for compensation.'

        - Some companies deliberately limit their exposure. Eg at least one password manager service has been hacked and some password managers 'limit the developer's liability to USD 100 per user. As a result, the significant potential costs for the users of a password manager are externalities for the developer. . . a password manager may store hundreds of passwords, whose breach could inflict costs on users far greater than the maximum USD 100 that is covered – this is a prime example of an externality a company makes their users bear.'
        - 'The lack of organisational liability for all the costs of a breach may limit the incentive to stop them.'
    - It explains **information asymmetries**[d] as: 'Stakeholders do not have full information about the risks they may face online, making it difficult to take informed decisions. In particular, it is hard for organisations to benefit from taking the right steps to avoid data breaches, because they cannot convey their level of data security to customers. This limits the incentive to invest in data security.' Eg when choosing a password manager, 'a user would have no way of knowing what security tools are used for the password manager, and how well they are implemented, making it difficult to choose the safest one.'
        - 'Issues of adverse selection and moral hazard arise from the asymmetric information.'
            - Adverse selection: 'Those with better information will be selective in how they participate in a market. In the used car market, without a means to signal if a used car is high-quality, only those with lower quality cars will sell, resulting in a market of lemons. In insurance markets, people understand their own risk better than the insurance company, which can also result in adverse selection, as those with higher risk may be more likely to take out insurance (and then, with a riskier pool of insured, premiums will rise accordingly).'
            - Moral hazard: 'Insurance may lead those with coverage to take less care because they do not bear the full cost of their actions. For instance, if one had a car insurance with no deductible, and no increase in premiums, then people would have less incentive to park their cars securely, or may even take more risk driving. This is known as moral hazard.'
            - 'Consider the example of an online retailer, who is worried about being hacked, and wants to take actions to protect the company from a data breach.
                - Assume the retailer decided to invest a significant amount to protect their users' information from hackers, as a means to compete with other online retailers who might be more vulnerable. How would they signal this credibly to users? They could point out they have not been hacked, but that does not mean they could not be hacked. If there is no way to signal it, there is no way to win more customers, and thus by adverse selection, the market would consist of retailers who have underinvested in security.
                - If the retailer is still worried about the risks of a data breach – not having invested in the optimal amount of cybersecurity, the company might instead choose protection through cybersecurity insurance (this would be an example of adverse selection – those most at risk are most likely to take insurance). Now moral hazard

[d] 'Asymmetric information arises when one party to an agreement or exchange has more information than the other about the object of the exchange. The classic example is the used car market. The seller of the car knows more about its quality, and how it has been treated, than the buyer. It is difficult, however, for the owners of high-quality cars to convince buyers that they are high quality, so cars that are the same on paper (model, year, mileage driven), will sell for the same average price. As a result, high-quality cars are less likely to be sold, and the market is full of low quality 'lemons'.'

can kick in – having the insurance means potentially investing even less in cybersecurity, because there is even lower cost from a breach, which of course becomes more likely.'

- Given these externalities, the USA's Congressional Research Service questioned whether leaving it to the self-interest of companies such as pipeline operators will result in a sufficient level of cybersecurity (eg for critical infrastructure) because it means: 'To a great extent, the public must therefore rely on the pipeline industry's self-interest to protect itself from cyber threats.'[6] Companies can be unwilling to provide more cybersecurity than the law requires (presumably because of cost and the externalities and information asymmetries above). Eg TalkTalk, a UK broadband provider, was hacked in October 2015 resulting in 157,000 unencrypted customer records being breached. This was their third security event in a row and still the TalkTalk CEO said '"[Customer data] wasn't encrypted, nor are you legally required to encrypt it…We have complied with all of our legal obligations in terms of storing of financial information."' Therefore the above indicates that leaving it to the companies to decide the level of security of their electronic transactions is likely to result in inadequate cybersecurity (which is what the examples below also show).
    - 'Apply encryption as the norm for data in transit and at rest . . . Internet Society believes encryption should be the norm for Internet communications and data. More specifically, organisations should use a level of encryption whose time and cost to crack, if at all possible, outweighs any possible benefits of an attacker potentially gaining access. Many of the case studies highlight the cost of a lack of encryption – Target, the Office of Personnel Management, and others had no encryption, while TalkTalk, Korea Pharmaceutical Information Center, and others used insufficient encryption. . . The economic reasons for limited or no encryption are two-fold – the cost of properly implementing strong encryption is perceived to be high, while the benefits are not perceived to be high enough.' ('Encryption involves encoding data so that only the intended parties can read them').
- Government intervention may be required in cybersecurity:
    - given the externalities and information asymmetries with the resulting adverse selection and moral hazard in cybersecurity, 'governments may need to intervene in certain cases to help convey certain attributes of security.' For example to know the quality of a car airbag when buying a new car, 'people may need to rely on a third party, such as the government, to test and certify the car meets minimum standards. . . For credence attributes [which one may never learn about], such as safety, a consumer or private third party agent may never be able to assess them. Governments may need to mandate safety standards. For instance, governments may be best placed to test-crash automobiles and ensure that they meet safety standards.'
        - 'In some cases, some minimum standards for data handling may need to be mandated if not voluntarily adopted (such as data security and data minimisation provisions in law). . .
        - where outside rating or certification is not sufficient, or where adequate voluntary standards are not fully adopted, a government mandate may be needed. This is particularly true where the market failure is significant – either high externalities, or extreme asymmetric information. Privacy and data protection laws usually contain minimum data security requirements. As noted above, there are examples where mandates are most suited to resolving a market failure.
    - 'organisations must be induced to internalise the negative externalities they cause other organisations and users, and society at large, to reduce the incentive to create them. In many cases, this can be monetary – just as taxes can reduce certain types of pollution, increasing the liability or penalty faced by the organisation responsible for allowing a breach to occur will no doubt lower the probability of one occurring. Just as some types of pollution are too toxic and must be outlawed, such as lead in paint or gasoline, there may be a need to impose certain data security practices outright.'

Other cybersecurity experts such as the special adviser to IBM Security agree: 'Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. ... the interests of the companies often don't match the interests of the people. ... Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks.'[7]

TPP, WTO, EUFTA and RCEP proposals

TPP

Article 14.6 of the Trans-Pacific Partnership[e] (TPP)[8] restricts governments from setting standards for the security of electronic transactions:

> '2. No Party shall adopt or maintain measures for electronic authentication that would:
>
> (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; . . .
>
> 3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.'

The TPP's ecommerce chapter has some minor exceptions, the chapter does not apply to:

- government procurement
- 'information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.'

WTO

The European Union (EU) has made a similar proposal at the World Trade Organization (WTO): the 2017 version also has an exception for 'a particular category of transactions',[9] but this exception is not present in the EU's 2018 WTO proposal[10]. There is currently no mandate to **negotiate** ecommerce rules at the WTO. At the WTO, the current mandate is merely to **examine** various ecommerce issues.[11] However, at the WTO Ministerial Conference in Buenos Aires from 10-13 December 2017 (MC11), some WTO Members signed a joint statement saying they 'will initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce'[12] and some meetings of this group have already been held in 2018.

EUFTAs

All EU free trade agreement (FTA) ecommerce proposals available in English on the EU's website (ie to Chile and Indonesia)[f] have the provision above, with no categories of exceptions[g] to the provision above (requiring it to be left to the private sector to determine the appropriate authentication method for the electronic transaction).

However this extreme proposal appears to be a bargaining position which the EU is willing to add exceptions to (presumably in return for concessions from the other country) in its concluded FTAs. For example:

---

[e] Now renamed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership text, but the ecommerce chapter is still the same as in the TPP, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/tpp-and-cptpp-the-differences-explained/ and https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/.

[f] Since the other EUFTA proposals at http://trade.ec.europa.eu/doclib/press/index.cfm?id=1395 do not currently include the ecommerce chapter, or are only available in French (to Tunisia).

[g] The EU proposes an exception to the ecommerce chapter as a whole for 'gambling services, broadcasting services, audio-visual services, services of notaries or equivalent professions and legal representation services', but does not include the exception for 'a particular category of transactions' which is in its 2017 WTO esignatures/eauthentication proposal.

- In the Japan-EUFTA, there is an exception for 'a particular category of transactions'.[13]
- in the Mexico-EUFTA, there is an exception where 'a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law. **Such requirements shall be objective, transparent and non-discriminatory and shall relate only to the specific characteristics of the category of transactions concerned**.'[14] This appears to limit the exception to one category of transactions and even that is further restricted by the bolded sentence requiring that the standards etc required for that one category of transactions must be objective, transparent and non-discriminatory and shall relate only to the specific characteristics of the category of transactions concerned. This limits the regulations possible even for the one category of transactions for which an exception is allowed and is more restrictive than the Japan-EUFTA.

RCEP

A similar proposal may have been made in the Regional Comprehensive Economic Partnership (RCEP) ecommerce negotiations.[h]

Https as an example of security

The difference between http and https

A website using http is not encrypted which means that anyone can see the information you give it (eg login details, passwords etc), as if it were passing through a transparent tube because it is clear text.[15]

If websites use http**s**,[i] this means it is encrypted so it is more difficult for third parties (eg thieves) to see credit card details a customer puts into a website to buy something online/book an airticket or hotel etc. Ie with https 'those tubes become opaque. Only people at the end can see what's traveling through them.'[16]

The benefits of switching to https

As noted above, using https means that when sensitive personal information such as credit card numbers is being transmitted, it cannot be read by others. Furthermore, 'Edward Snowden's NSA leaks also made clear how much unencrypted data the NSA was siphoning en masse from the internet, renewing people's interest in protecting their connections.'[17]

https also protects '"the right to read in private." A visitor to Wikipedia might be learning about a medical condition they may suffer from. Someone searching Craigslist at their office could be looking for a new job. A student reading the Washington Post might be following transgender political issues. All of those activities, Eckersley argues, deserve to be protected from an internet provider, employer, or school administrator just as much as the person's credit card number.'[18]

'In fact, HTTPS protects more than confidentiality. It also offers authentication and what website administrators call "integrity."

- For a site to register in a browser as HTTPS encrypted—noted with a padlock in the browser's address bar—it needs to **authenticate** itself: to prove that it's the site it says it is, rather than an impostor. To do that, a website's administrator asks a "certificate authority" company like Comodo or Symantec to issue the site a "certificate," which says that the public encryption key associated with the site really does belong to the site. Though certificate authorities have occasionally been hacked, like in the case of the Dutch firm Diginotar in 2011, breaking that system of trust. But in general, a certificate means that when your browser says you're at https://google.com, you really are sharing your data with a Google server and no one else.
- As for "**integrity**," HTTPS also prevents any interloper on your local network from tampering with or partially blocking the contents of a site on its way from a server to your browser. Without

[h] Since the leaked terms of reference for the RCEP ecommerce chapter include an electronic signature item, http://bilaterals.org/?rcep-draft-e-commerce-chapter.

[i] 'HTTPS (Hyper Text Transfer Protocol **Secure**) appears in the URL when a website is secured by an SSL certificate', https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https

HTTPS, a government censor can choose to block certain pages of a site or even just parts of a page. More active tampering could allow an internet service provider to insert ads or hackers to inject code designed to compromise your computer.'[19]

Given the way that data sent via mere http can easily be intercepted, the manager of application security research of the company which found the dating app vulnerability (see below) said 'There's really no excuse for using HTTP these days'.[20]

The costs of switching to https

There are one-off[j] and ongoing costs to switching from http to https.[21] For example websites using Amazon's cloud services have to pay more on an ongoing basis for a https website.[22] (Amazon has 35% of the cloud worldwide market share, the most of any company[23]).

How common is https?

Given the switching costs, many businesses will not switch to https without being required to by a government (eg for consumer protection reasons, see below). For example:

- One study cited in 2016 of '540 UK B2B businesses showed that the uptake of switching to HTTPS was in the 2 to 3 percent range'[24]
- A March 2016 study 'showed that 79 of the 100 most highly trafficked websites on the internet still do not yet use HTTPS encryption.'[25]

'"Most users still don't know about HTTPS, and even if they do, they don't have any control over it. They have to either transmit their data in the clear or go somewhere else," says Aas. "If we're going to protect those people, we need to get websites to adopt HTTPS ... It's really a lynchpin in the internet's security right now."'[26]

Since users/consumers cannot force websites to use https, they are forced to send their data unencrypted or not use that service. This is a reason why governments may need to regulate to require the use of https (eg for certain types of sensitive data, see below).

Some examples of where government regulation of electronic transactions to ensure their security exist/may be needed

Governments may need to make sure electronic transactions are secure from being hacked in a number of situations. Some of these are below. The government regulations below (and those which may be needed in the situations below) would not be possible if the eauthentication proposals above are agreed to (or only possible for one category of transactions if that exception is allowed), unless other exceptions are agreed.

The examples below were found from a search for a few hours and new examples occur every week given the rapid speed of technological change Therefore by the time any ecommerce negotiations have concluded, many more exceptions are likely to be needed, including in currently unforeseen sectors/regulations.

Agreeing to restrictions on governments' ability to set authentication methods for electronic transactions in trade agreements (which are usually difficult to update/amend because they require the consent of all the countries involved) would lock-in restrictions/prohibitions on the ability to regulate in a fast-changing field where the need for regulation is already clear and likely to increase.

Privacy laws

Regulations in the US state of Massachusetts require 'Encryption of all transmitted records and files containing personal information[k] that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly' that is about a Massachusetts resident.[27]

[j] Eg the high cost of secure certificates, https://www.wired.com/2011/03/https-is-more-secure-why-isnt-the-web-using-it-today/

The US state of Nevada specifies that data collectors[l] can only transfer personal information[m] electronically if 'the data collector uses encryption to ensure the security of electronic transmission' (except for faxes and voice calls).[28]

Many other US states have enacted industry-neutral laws regulating the transmission of personal information.[29]

Private sector transmission of social security numbers (SSNs) etc

The problem

'Since the creation of the SSN in 1936, the private sector increasingly has utilized it for various purposes – both as an identifier and an authenticator – because it is the only permanent, unique piece of information that most Americans have about themselves. The SSN's use has expanded as organizations have adapted their business and record-keeping systems to utilize increasingly sophisticated automated data processing. The SSN has, over time, become an integral part of our financial system.

As the private sector's use of the SSN has grown, so too has its availability and value for identity thieves.'[30]

Identity theft based on social security numbers (SSNs)[n] is such a big problem in the USA, multiple US government websites have warnings about it such as:

- With a person's name and social security number, 'an identity thief could open new credit and bank accounts, rent an apartment',[31]
- access existing accounts, or obtain government benefits in the consumer's name.[32]
- 'use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.'[33]
- Identity thieves can use your SSN to get your tax refund from the Internal Revenue Service (IRS): 'If you're eligible for a refund, a thief could file a tax return before you do and get your refund. Then, when you do file, the IRS will think you already received your refund.'[34]

Businesses will continue to use SSNs

---

[k] is defined as 'a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account;'

[l] defined to include a 'corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.'

[m] Defined to be a human being's first name/'first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

(a) Social security number.

(b) Driver's license number, driver authorization card number or identification card number.

(c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

(d) A medical identification number or a health insurance identification number.

(e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.'

[n] According to the US government's Federal Trade Commission: 'the SSN facilitates identity theft, i.e., that it is a necessary, if not necessarily sufficient, data element for many forms of this crime to occur', https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

Businesses can ask for a person's SSN[35] as they routinely rely on SSNs to ensure accurate matching of consumers with their information within organizations and that the information they use or share with other organizations is matched to the right individual.[36] For example it is used to 'share patient records within the health care system'.[37]

'Many businesses contend that the SSN is superior to any other item of information currently available to identify consumers and link information to them. Commenters from various sectors of the economy asserted that there are no other identifiers that are as reliable, cost-effective, and accurate for data matching as SSNs, because only the SSN is permanent, unique, ubiquitous, and common across organizations.'[38]

'And you may be denied service if you don't give the number.'[39]

Unsurprisingly, a US citizen's social security number is very valuable (eg on the dark web).[40] This is because it is widely used by companies and 'Over the decades, the Social Security number became valuable for what could be gained by stealing it, said Bruce Schneier, a fellow at Harvard's Kennedy School of Government. It was the only number available to identify a person and became the standard used for everything from confirming someone at the doctor's office to school. . . The failure of the Social Security number is that there's only one for each person, "once it's compromised one time, you're done," Bob Stasio, a fellow at the Truman National Security Project and former chief of operations at the National Security Agency's Cyber Operations Center.'[41]

Identity theft via SSNs was already such a problem in 2008 that the US government's Federal Trade Commission wrote a report on it recommending:[42]

- 'limiting the circumstances and means by which they can be transmitted, would make it more difficult for thieves to obtain SSNs, without hindering their use for legitimate identification and data matching purposes'
- 'that measures be taken to reduce the unnecessary display and transmission of SSNs and improve data security. With respect to its central proposals – improving authentication, reducing unnecessary SSN display and transmission, improving data security, and requiring breach notification – the Commission recommends that Congress consider establishing national standards that would be delineated further through agency rulemaking. In addition, the Commission recommends that Congress consider granting it authority to obtain civil penalties for violations of these rules.'
- 'The Commission recommends that Congress consider creating national standards for the public display and the transmission of SSNs. Federal legislation would establish a nationwide approach to reducing unnecessary display and transmission of SSNs, while addressing concerns about a patch-work of state laws with varying requirements. National standards should prohibit private sector entities from unnecessarily exposing SSNs. The precise standards should be developed in rulemaking by appropriate federal agencies (i.e., agencies that oversee organizations that routinely transmit or display SSNs), and should include, for example, prohibitions against:
    - . . . transmitting (or requiring an individual to transmit) an SSN over the Internet, unless the connection is secure from unauthorized access, e.g., by encryption or other technologies that render the data generally unreadable'

In the wake of the massive Equifax data breach of 2017, Rob Joyce, special assistant to the president and White House cybersecurity coordinator said the use of social security numbers as the main method of assuring people's identities is '"a flawed system that we can't roll back that risk after we know we've had a compromise," he said. "I personally know my Social Security number has been compromised at least four times in my lifetime. That's just untenable."' [43]

However to change away from the social security number system is not easy, '"You'd need to change a lot of existing public law," Rotenberg said. "There would need to be extensive hearings and study about the consequences. It's a complicated issue."'[44]

Some governments have passed laws to address this problem

In the meantime, approximately 25 US states have passed laws limiting the public display and/**or** use of SSNs such as California[45] and Minnesota[46] which have laws regulating how social security numbers can be transmitted. They specify that private companies cannot require:

- a person to transmit their Social Security number over the internet, unless the connection is secure or the Social Security number is encrypted (with some exceptions).
- A person to use their Social Security number to access a website unless a password or unique personal identification number or other authentication device is also required to access the website.

  These would be prohibited under Art 14.6.2 TPP unless the exception for a particular category of transactions is used (or another exception applies).

Healthcare transactions

Under the USA's Health Insurance Portability and Accountability Act (HIPAA) electronic transactions (a transaction is 'an electronic exchange of information between two parties to carry out financial or administrative activities related to health care',[47] eg a hospital sending a claim to the health insurance company to be paid for a patient's operation) between HIPAA covered entities must use certain standards.[48] Since these standards (x12) appear to be covered by the definition of electronic authentication in Art 14.1 TPP, this is not permitted by the TPP unless the exception for a particular category of transactions in Art 14.6.3 is used or the (difficult to use,[o] see below) TPP general exceptions[49] for health, environment and privacy apply.

The USA's Patient Protection and Affordable Care Act also requires compliance with operating rules ('defined as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications."'[50]). 'Operating rules set certain requirements for transactions that are covered by HIPAA. They specify the information that must be included when conducting standard transactions, making it easier for providers to use electronic means to handle administrative transactions.'[51] This is also not permitted by the TPP unless the exception for a particular category of transactions in Art 14.6.3 is used or the (difficult to use,[p] see below) TPP general exceptions[52] for health, environment and privacy apply. However the stated rationale (see below) re efficiency and reducing costs is not one of the TPP's general exceptions.

The rationale for the US government setting these national standards and operating rules includes:[53]

- 'To reduce paperwork and streamline business processes across the health care system'
- 'ensuring the health care community reaps the benefits of standardized transactions and reduced administrative costs.'
- 'Standard transactions, operating rules, code sets, and unique identifiers allow information to be shared electronically in consistent ways.
- With common standards for content and formats, information moves quickly as it is shared between providers and health plans in predictable ways.
- These standards have the potential to decrease health costs, time spent on paperwork, and administrative burden, giving providers more time for patient care.
- And quick communications with insurers can help inform patients upfront about coverage, benefits, and out-of-pocket costs.'

---

[o] They incorporate the GATT and GATS health and environment etc exceptions which countries have tried to use 44 times at the WTO and succeeded once, https://www.citizen.org/sites/default/files/general-exception_4.pdf.

[p] They incorporate the GATT and GATS health and environment etc exceptions which countries have tried to use 44 times at the WTO and succeeded once, https://www.citizen.org/sites/default/files/general-exception_4.pdf.

- Reducing the $billions on healthcare administration alone the USA spends every year by making it more efficient so hospitals and insurance companies etc can share information electronically.[54]
- That eligibility for health insurance and claims status can be checked online, eg allowable charges. The information and the way it is transmitted is more uniform, so hospitals can just use one kind of electronic request for all health insurers[55]

The USA also has mandatory operating rules for electronic funds transfer (EFT – ie the payment a health insurance company pays to the hospital's bank account) and electronic remittance advice (ERA).[56] ERA is what health insurance sends to the hospital to explain what the payment is for. The rules set a standard format and data content for every transaction's EFT and ERA which automates payment reconciliation for providers and simplifies the process. This is also not permitted by the TPP unless the exception for a particular category of transactions in Art 14.6.3 is used or the (difficult to use,[q] see below) TPP general exceptions[57] for health, environment and privacy apply. However the rationale above re simplifying the process is not one of the TPP's general exceptions.

This indicates that leaving it to the private sector (as occurred before the US regulations above) led to multiple private sector standards being required which reduced efficiency and interoperability and caused high administrative costs. The US government therefore thought the benefits outweighed the costs in requiring a single national standard to improve efficiency and reduce costs. This kind of regulation would not be possible under the ecommerce proposals above (except for those with an exception for a particular category of transactions, if this is the one category selected). Any health exception applying to these proposals (see exceptions below) would not be relevant here since these mandatory standards were introduced by the government to increase efficiency and reduce costs, not for health reasons (even though the regulations apply to the healthcare sector).

Online banking

The problem

Online banking needs to be secure. This is because when it is left to the banks, banking apps and online banking are often surprisingly insecure. Eg:

- 'In 2014, Ariel Sanchez tested 40 home banking apps and found that 90% included insecure links (ones that didn't use SSL), 40% didn't check the validity of SSL certificates, 50% were vulnerable to cross-site scripting, and 40% were vulnerable to man in the middle attacks. . . Today's banking apps should be much more secure, but I wouldn't bet on it. . . Whatever device you are using, the best solution is end-to-end encryption, shown by "https" addresses and a padlock in the browser.'[58]
- even British banks in December 2017 were taking shortcuts (presumably to save money and effort) and using mere http on the front page of the bank's website, however security experts note 'without HTTPS an attacker could theoretically modify elements of a bank's website. They could send victims to a fake online banking site and steal their information. "The homepage is insecure so you can't trust anything on it," said Mr Hunt. "This is a banking website. No excuses," added Stephen Kellett, from security firm Software Verify. "All pages, whether performing transactions, the homepage, the about page, the whole lot, they should all be secure. Why? Because they all launch the login page."'[59]

Governments are already requiring a certain level of security

Given problems such as those above, a number of financial regulators already specify the level of security of online banking transactions. For example:

[q] They incorporate the GATT and GATS health and environment etc exceptions which countries have tried to use 44 times at the WTO and succeeded once, https://www.citizen.org/sites/default/files/general-exception_4.pdf.

1) The Malaysian central bank therefore requires two-factor authentication etc for online banking.[r]

2) The Indian central bank specifies that 'Banks providing mobile banking services shall comply with the following security principles and practices for the authentication of mobile banking transactions:

   a) All mobile banking transactions shall be permitted only by validation through a two factor authentication.

   b) One of the factors of authentication shall be mPIN or any higher standard.

   c) Where mPIN is used, end to end encryption of the mPIN is desirable, i.e. mPIN shall not be in clear text anywhere in the network.

   d) The mPIN shall be stored in a secure environment.'[60]

Financial regulators in other countries may have similar requirements.

Financial entities

New York State Department of Financial Services passed a new regulation which came into force on 1 March 2017 in response to cybersecurity threats to the financial services industry. Its requirements include:

- companies authorised under the Banking, Insurance, or Financial Services Law to encrypt nonpublic information[s] held or transmitted by these companies both in transit over external networks and at rest (unless it is not feasible).[61]
- Multi-factor authentication[t] for any individual accessing the internal networks of companies authorised under the Banking, Insurance, or Financial Services Law from an external network, unless the company has approved in writing the use of reasonably equivalent or more secure access controls.[62]
    - Whether this is an example of 'parties to an electronic transaction' (eg under the TPP's electronic authentication provision[63]) depends on how 'parties' and 'electronic transaction' are defined (they are not defined in the TPP text). Eg whether an employee logging in remotely to her bank's internal database to work from home is a different 'party' to the bank and this working remotely is an 'electronic transaction'. The TPP countries may have agreed what 'parties' and 'electronic transaction' mean in the TPP's negotiating history,[u] however this has not been released, so only the TPP governments know whether this type of situation would be covered by Art 14.6 TPP.

---

[r] 'To further strengthen the safety of Internet banking services, all banking institutions offering Internet banking services are required to implement two-factor authentication for Internet banking transactions. The second authentication factor is to complement the username and PIN or password (which is the first factor authentication) by way of using an additional authentication tool such as transaction authorisation code (TAC), digital certificate, smart card or USB token, or a customer's own biometric characteristic such as fingerprint or retinal pattern. The second authentication factor is required for high-risk transactions such as registering new payees or beneficiaries, third party funds transfer, payment to unregistered parties, prepaid airtime reloads, bill payments and changing confidential information like correspondence address and contact numbers.' http://www.bnm.gov.my/files/publication/fsps/en/2006/cp04.pdf

[s] This includes healthcare information and name + '(i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records'

[t] Defined as 'authentication through verification of at least two of the following types of authentication factors:
(1) Knowledge factors, such as a password; or
(2) Possession factors, such as a token or text message on a mobile phone; or
(3) Inherence factors, such as a biometric characteristic.'

[u] This negotiating history is binding between the Parties because of Article 32 of the Vienna Convention on the Law of Treaties (VCLT) which specifies that 'the preparatory work' of the treaty can be used to confirm the meaning of a term or determine the meaning of a term when it is ambiguous or obscure,

Credit/debit card data

The US government's Federal Trade Commission (FTC)[64] has charged companies which failed to encrypt sensitive data (eg credit/debit card information) in transit with being unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[65] For example:

- TJX has 2,500 stores worldwide. It collected credit/debit card information and other personal information and transmitted it unencrypted (in clear text) within and between its stores. An intruder connected to TJX's networks 'without authorization, installed hacker tools, found personal information stored in clear text, and downloaded it over the internet to remote computers. Further, between May and December 2006, an intruder periodically intercepted payment card authorization requests in transit from in-store networks to the central corporate network, stored the information in files on the network, and transmitted the files over the internet to remote computers. . . The breach compromised tens of millions of unique payment cards used by consumers in the United States and Canada. To date, issuing banks have claimed tens of millions of dollars in fraudulent charges on some of these accounts.'[66] The FTC charged TJX with 'unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a)'[67] and TJX settled.[68]
- BJ's 'operates 150 warehouse stores and 78 gas stations in 16 states in the Eastern United States. Approximately 8 million consumers are currently members, with net sales totaling about $6.6 billion in 2003.' BJ did not provide reasonable security for this sensitive data including because it 'Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores'.[69] 'fraudulent purchases were made using counterfeit copies of credit and debit cards the banks had issued to customers who had used their cards at BJ's. This was possible because their customer names, card numbers and expiration dates from their cards were stored on BJ's computer networks and then illegally accessed and used on 'counterfeit copies of cards that were used to make several million dollars in fraudulent purchases.'[70] After this, the FTC charged BJ's with unfair practices and BJ settled.[71]

Nevada has privacy protection system for companies doing business in Nevada which accept a credit/debit card which requires them to comply with the current version of the Payment Card Industry (PCI) Data Security Standard (PCIDSS).[72]

Implications of the private sector choosing the appropriate authentication method for credit/debit card transactions

The dominant companies set the standards and penalise those who do not comply

The PCIDSS is a private sector standard set up in 2006[73] by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc[74] which has a number of requirements including to 'Encrypt transmission of cardholder data and sensitive information across open public networks'[75] and multifactor authentication 'for remote access (originating from outside a company's network) where that remote access could lead to access to the cardholder data environment.'[76]

A US restaurant run by the McCombs was fined US $90,000 by Visa and Mastercard for allegedly violating the PCIDSS requirements that were introduced four years after they signed their contract with the bank and were only referred to on a website printed on bank statements that because they did online banking they did not notice. Although it was their bank who was fined by Visa and Mastercard, the banks have contracts with the retailers which force the retailers/restaurants to repay the banks for any fines they have to pay Visa/Mastercard. This fine was imposed even though most of the fraudulent activity reported involved credit card numbers that had never been used at the restaurant

---

https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf. Countries that are party to the VCLT are bound by it. Furthermore, Articles 31 and 32 of the VCLT reflect customary international law (International Court of Justice in *Libya v Chad*, ICJ Reports (1994), page 4 para 41) and customary international law is binding on all countries, even those which are not party to the VCLT.

and the retailer/restaurant cannot appeal it (only the bank can who has no incentive to do so as they just pass the fine through to the retailer/restaurant and it costs the bank an unrefundable US $5,000 to appeal).[77]

This controversial PCIDSS 'system, imposed on merchants by credit card companies like Visa and MasterCard, has been called a "near scam" by a spokesman for the National Retail Federation and others who say it's designed less to secure card data than to profit credit card companies while giving them executive powers of punishment through a mandated compliance system that has no oversight. "It's just like Visa and MasterCard are governments," said Stephen Cannon, an attorney representing the McCombs. "Where do they get the authority to execute a system of fines and penalties against merchants? . . . The McCombs assert that the PCI system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties. Visa and MasterCard impose fines on merchants even when there is no fraud loss at all, simply because the fines "are profitable to them," the McCombs say.'[78]

For example, Heartland had to pay US $139 million to the credit card companies and in legal fees when it was breached.[79]

Furthermore, since Visa and Mastercard have 80% of the market share,[80] retailers and restaurants etc have no choice, they have to use Visa and Mastercard and therefore their PCIDSS system.

As the Michaels chain (with 1,000 stores) noted, the PCIDSS 'council is set up so that credit card companies and banks retain all power over the ultimate mandates, fines, and anything else connected to PCI. Because of this, the mandates do not represent what is the ``best'' security, but rather what is best for the credit card companies and their financial institution partners. . . It is not an industry standards body. . . All of this arises from rules that initially grew from a card monopolist that we have no choice but to do business with or risk the loss of a large portion of our business. It would be impossible for a retailer like Michaels to survive without taking Visa. So we, like other retailers, swallow the tens of millions we have spent to become PCI-compliant, in many cases unnecessarily spent, which both reduces profitability and increases the costs of everything we, the merchant, sells.'[81]

The USA's National Retail Federation, the world's largest retail association representing 'an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees--about one in five American workers--and 2008 sales of $4.6 trillion' noted in a US House of Representatives hearing that 'the PCI guidelines are onerous, confusing, and constantly changing. Many retailers say that basic compliance is like trying to hit a rapidly moving target.'[82]

The dominant companies set a standard that is difficult and expensive to comply with

It is difficult and expensive to comply with PCIDSS as even a US $4 billion chain with 1,000 stores testified to the US Congress: 'The PCI data and security standards are an extraordinarily complex set of requirements; they are very expensive to implement, confusing to comply with, and ultimately subjective both in their interpretation and in their enforcement. The program is rife with ambiguity and complexity.'[83]

An ecommerce provision which requires parties to an electronic transaction to be able to 'mutually determine the appropriate authentication methods for that transaction' enables the Visa/Mastercard/American Express privatised lawmaking and penalties to continue as above and retailers/restaurants have little choice since they almost all have to offer the ability to pay by Visa/Mastercard/American Express to their customers. Therefore even if a restaurant did not want to comply with the PCIDSS standard, so it was not 'mutually determined', it has little choice.

The private sector standard is not secure enough

As the US $4 billion Michaels chain store testified to the US Congress: 'PCI states that all credit card data must be encrypted. There is an exception to this requirement, however; PCI states that data traveling over a private network need not be encrypted. While a private network is more secure, I still would not choose to send credit card numbers through this number unencrypted. Why? Because it adds unnecessary risk. However, the credit card companies' financial institutions do not accept encrypted transactions. We at Michaels have asked, for the past 3 years, for the ability to send

encrypted information to the bank. To date, this has not happened. Why is this an issue? One might ask the consumers affected by the Heartland Payment Systems data breach, or TJX Corporation, for that matter. It has been suggested that methods used in those breaches capitalized on this flaw. . . The criminals used a ``Trojan Horse'' that read the credit card data ``in flight.'' This is not the stored data I spoke of earlier, but rather the numbers that were flowing through the communication channel for approval. One reason thieves could capture this data is because it was not encrypted. Had it been encrypted they would most likely not have been able to read the data.'[84]

In 2010, more than a year after this problem was raised in a US Congressional hearing, this was still a concern in an article analysing the massive Heartland breach when hackers accessed 130 million credit card numbers: 'A potential weakness lies in the fact that data must be decrypted to move from Heartland's system to Visa and MasterCard, as credit card companies accept only unencrypted data.'[85]

Furthermore there are concerns that PCIDSS is not sufficiently secure. Eg the US House of Representatives Committee on Homeland Security was concerned that 'a number of well-known companies have experienced massive data breaches in their internal computer networks, resulting in the compromise of sensitive customer data. The criminals who perpetrated these intrusions targeted the credit and debit card account information held by merchants or third-party data processors as the result of retail transactions . . . We know that some percentage of the fraudulent charges and illicit businesses from these activities is used to fund terrorist activity throughout the world.'[86] The Chair of this Committee 'launched an investigation to determine whether the PCI standards have been effective in reducing cybercrime. The results of this investigation suggest that the PCI standards are of questionable strength and effectiveness.'[87]

'The effort to become PCI-compliant is a daunting challenge for merchants whose core competency is the selling of merchandise rather than expertise in security. The cost for the largest merchants can be as high as $18 million a year. Many believe that if they complete this arduous task, they will be rewarded with a secure system. But the committee's investigation confirms what many analysts have known for years. In the words of one credit card company, full compliance with the PCI standard does not guarantee that the merchant or vendor will not be the victim of a data breach.

Take last year's data breach of Hannaford Brothers Company, for example. Hackers installed malicious code on servers to every one of the grocery stores in the Hannaford chain. The malware intercepted the data stored on the magnetic stripe of payment cards as customers used them at the checkout counter. Hannaford received certification that they were PCI-compliant on February 28, 2008. But on February 27, 2008, according to the documents obtained by the committee, Hannaford was notified that a number of the credit card numbers from its network were stolen and being used on the black market. In other words, Hannaford was being certified as PCI-compliant while an illegal intrusion into its network was in progress.'[88]

The USA's National Retail Federation, the world's largest retail association noted in a US House of Representatives hearing that 'PCI is little more than an elaborate patch . . .' PCI protocols have required many merchants to scrap good existing data security programs and replace them with different security programs that meet PCI rules that aren't necessarily any better. Even companies that have been certified as PCI-compliant have been compromised.

Unfortunately, the economic incentives for the card companies to remedy these flaws in their system have been diminished. It appears to our industry that the credit card companies are somewhat less interested in improving their product and procedures than they are in reallocating their fraud costs. In our view, if you peel back the layers around PCI, you will see it for what it really is, a tool to shift risk off the banks and credit cards' balance sheets and place it on others. It is their payment card system, and retailers, like consumers, are just users of their system.' [89]

Before agreeing to these eauthentication rules which continue to allow the PCI system, have the governments consulted retailers, restaurants/their industry associations etc?

Whatsapp

Canada's Office of the Privacy Commissioner investigated Whatsapp and its 2013 report found that:[90]

- 'WhatsApp's account confirmation messages were being sent using ordinary web traffic ports, allegedly without encryption or safeguards. Absent appropriate security measures, confirmation messages and any personal information attached thereto ran the risk of being intercepted. Once intercepted, a confirmation number could be used to access and receive a user's messages and/or any other personal information sent to the programmed number'
- 'At the time that our investigation was initiated, messages sent using the application were not encrypted. As such, messages sent and received using the application ran the risk of interception, especially where a user elected to use the service through unprotected Wi-Fi networks. In the course of our investigation we confirmed that messages sent between application users were not secure. Even in cases where data was sent over ports used for secure https (SSL/TLS) communications, personal data including the content of user messages and telephone numbers were clearly visible. . . In its representations to our Office, WhatsApp confirmed that messages sent and received using the application were not being encrypted – affirming the need to introduce safeguards to ensure the security of instant messages and any other personal information attached to those messages. In partial response to our concerns, in September 2012 WhatsApp began adding protocol encryption to its mobile messaging service. If properly applied, the end-to-end encryption would appropriately safeguard messages from eavesdropping or interception.'

Uber

Uber stored consumer information 'in a third-party cloud storage service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). Uber stores in the Amazon S3 Datastore a variety of files that contain sensitive personal information, including full and partial back-ups of Uber databases. These back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, email addresses, phone numbers, driver's license numbers, and trip records with precise geolocation information.'[91]

Uber failed to require multi-factor authentication to the Amazon S3 Datastore.[92] As a result of these and other failures, 'intruders accessed Uber's Amazon S3 Datastore multiple times using access keys that Uber engineers had posted to GitHub, a code-sharing site used by software developers. First, on or about May 12, **2014**, an intruder accessed Uber's Amazon S3 Datastore using an access key that was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore (the "2014 data breach"). The intruder accessed one file that contained sensitive personal information belonging to Uber Drivers, including over 100,000 unencrypted names and driver's license numbers, 215 unencrypted names and bank account and domestic routing numbers, and 84 unencrypted names and Social Security numbers.'[93]

Presumably Uber sending sensitive personal information (and partial back-ups of Uber databases) to Amazon's cloud storage service would be 'parties to an electronic transaction' and so covered by the proposed ecommerce rules, see above.

After this 2014 breach, the New York Attorney General required Uber to encrypt GPS-based location information when in transit and the adoption of multi-factor authentication, or similarly protective access control methodologies.[94] Since Uber database back-ups included geolocation information[95] and Uber backing up its data to Amazon's cloud are presumably 'parties to an electronic transaction' (see above), then the New York requirement for this to be encrypted appears to be the government intervening (assuming 'Party' is defined to include subnational governments[v]) to set a performance standard and preventing Uber and Amazon from determining the appropriate authentication method for this transaction. This New York requirement would therefore not be permitted under the ecommerce proposals (unless it is the one category permitted as an exception in some ecommerce proposals).

Then 'between October 13, **2016** and November 15, 2016, intruders accessed Uber's Amazon S3 Datastore using an AWS access key that was posted to a private GitHub repository ("the 2016 data

[v] It is assumed throughout this note that subnational governments are strictly bound by these ecommerce rules. Whether this is actually the case depends on the text in the trade agreement.

breach"). Uber granted its engineers access to Uber's GitHub repositories through engineers' individual GitHub accounts, which engineers generally accessed through personal email addresses. Uber did not have a policy prohibiting engineers from reusing credentials, and did not require engineers to enable multi-factor authentication when accessing Uber's GitHub repositories. The intruders who committed the 2016 breach said that they accessed Uber's GitHub page using passwords that were previously exposed in other large data breaches, whereupon they discovered the AWS access key they used to access and download files from Uber's Amazon S3 Datastore. The intruders downloaded sixteen files that contained unencrypted consumer personal information relating to U.S. Riders and Drivers, including approximately 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver's license numbers.'[96]

If Uber employees accessing GitHub repositories are 'parties to an electronic transaction' (which they appear to be), then the New York requirement for multifactor authentication appears to be the government intervening (assuming 'Party' is defined to include subnational governments) to set a performance standard and preventing Uber employees and Github from determining the appropriate authentication method for this transaction. This New York requirement would therefore not be permitted under the ecommerce proposals (unless it is the one category permitted as an exception in some ecommerce proposals).

Pipeline security

Cyberattacks are already occurring on oil and gas pipelines and their related companies, some have already been successful and regulators are already calling for mandatory standards. If governments cannot require a certain level of security for electronic transactions (due to these ecommerce rules in trade agreements), this can leave oil and gas pipelines etc vulnerable to cyberattacks.

Cyberattacks on pipelines are already occurring

Oil and gas pipelines are already often the target of cyberattacks. Eg:

- the trans-Alaska pipeline gets an average of 22 million cyberattacks per day and 'The rate of cyberattacks has roughly doubled in the last five years'.[97] 'Last year, the Department of Homeland Security and the FBI issued a warning that sophisticated cyberattackers have targeted the U.S. energy sector.

The USA's Congressional Research Service (CRS)[w] in a 2012 report on pipeline security noted that:[98]

- 'Over 500,000 miles of high-volume pipeline gather and transport natural gas, oil, and other hazardous liquids across the United States. In addition, nearly 900,000 miles of smaller distribution pipeline deliver natural gas to businesses and homes. This vast pipeline network is integral to U.S. energy supply and has links to power plants, refineries, airports, and other critical infrastructure. While pipelines are an efficient and fundamentally safe means of transport, many carry volatile, flammable, or toxic materials with the potential to cause public injury and environmental damage. Consequently, pipeline systems have drawn attention as possible targets for terrorism or other malicious activity.'
- the USA's network of natural gas and hazardous liquid pipelines 'is vulnerable to cyber attacks. In particular, cyber infiltration of supervisory control and data acquisition (SCADA)[x] systems

[w] The CRS was established by legislation in 1914 and does research for Members of the US Congress as part of the Library of Congress (an agency of the legislative branch of the U.S. government), https://www.loc.gov/crsinfo/about/, https://www.loc.gov/crsinfo/about/history.html, https://www.loc.gov/about/general-information/.

[x] 'Supervisory control and data acquisition (SCADA) systems are software-based industrial control systems used to monitor and control many aspects of network operation for railways, utility power grids, water and sewer systems, and pipeline networks. In the pipelines sector, SCADA systems collect data (e.g., line pressure) in real time from sensors throughout a pipeline network, displaying those data to human operators in remote network control rooms. These operators can send computerized commands from SCADA workstations to control geographically dispersed pipeline equipment such as valves, pumps, and compressor stations. The SCADA system

could allow successful “hackers” to disrupt pipeline service and cause spills, explosions, or fires—all from remote locations.

- In March 2012, the Department of Homeland Security (DHS) reported ongoing cyber intrusions among U.S. natural gas pipeline operators. These intrusions have heightened congressional concern about cybersecurity in the U.S. pipelines sector.’
- ‘Changes to pipeline computer networks over the past 20 years, more sophisticated hackers, and the emergence of specialized malicious software have made pipeline SCADA operations increasingly vulnerable to cyber attacks.’ This is ‘due to improvements in computer technology and the ongoing development of communications and Internet-based control system applications, SCADA systems have become much more vulnerable to outside intrusion and manipulation. Specific SCADA security weaknesses include the adoption of standardized control system technologies with known vulnerabilities, increased connection to external networks, insecure communication connections’
- ‘such cyber attacks could potentially disrupt pipeline service, damage pipeline equipment (e.g., with excessive pressure), or cause a hazardous release of pipeline commodities into the environment. Even if a hacker did not intend to damage or disrupt the pipeline system, by gaining access to or control of the SCADA system, the intruder could cause serious harm unintentionally.’
- ‘SCADA-related problems were a primary cause or contributing factor in several recent pipeline accidents which had catastrophic consequences.’ The report details the SCADA-related problems which have killed 11 people, spilled 819,000 gallons of crude oil into a river and caused $45million in damages etc. While these were accidents, they give an idea of the consequences of a successful cyberattack on SCADA systems used with pipelines.
- There recently has been a coordinated series of cyber intrusions specifically targeting U.S. pipeline computer systems.’
- an Al Qaeda video obtained in 2011 by the Federal Bureau of Investigation (FBI) reportedly called for “electronic jihad” against U.S. critical infrastructure.
- ‘Whether the self-interest of pipeline operators is sufficient to generate the level of cybersecurity appropriate for a critical infrastructure sector is open to debate. If Congress concludes that current voluntary measures are insufficient to ensure pipeline cybersecurity, it may decide to provide specific direction to the TSA to develop regulations and provide additional resources to support them’

Jim Guinn leads the company Accenture's cybersecurity business for the energy, utilities, chemicals and metals and mining industries. Guinn said that as far as he's concerned, the potential consequences of a major cyberattack should be the No. 1 thing keeping energy executives up at night — if it isn't already.

"It could be anywhere from a spill, to loss of the command of the plant itself, to explosion, to loss of life," he said. "It would be no different than losing a platform in the Gulf of Mexico or in the North Sea." . . . "The reality is, as long as these assets are attached to networks and they are managed the way that they are today, there is a real threat that they could be manipulated for malintent," Guinn said. "It's just the unfortunate world that we live in."’[99]

James Steffes, the executive vice president of Direct Energy Inc., which distributes electricity, also uses Energy Services said ‘“As we’ve become more digital, we’re going to see more and more threats,” Steffes said. “Bad people trying to do bad things” will continue to pose a threat to web-based services. “We’ll never be able to take our eyes off this ball because it’s just the nature of a digital environment.”

---

provides continuous feedback about conditions all along a pipeline, generating safety alarms when operating conditions fall outside prescribed levels.’

Natural gas systems and power grids have been increasingly going electronic as aging infrastructure is updated. Hackers are developing a penchant for attacks on energy infrastructure because of the impact the sector has on peoples' lives, said Scott Coleman, director of marketing and product management at Owl Cyber Defense, which works with oil and gas producers. If a hacker shuts down an electric substation, 20,000 people can be affected, he said.'[100]

The hacking of ESG

In April 2018, the electronic data interchange system that digitally processes customer transactions for a major pipeline network in the USA suffered a cyberattack and was shutdown.[101] The data firm which was hacked, Energy Services Group (ESG)'s 'electronic systems help pipeline operators speed up tracking and scheduling of gas flows. The company also supplies electricity prices and demand models that retail power providers depend on to bill homes and businesses, and determine how much supply to secure for customers in wholesale markets.'[102] 'The electronic systems that were targeted in the recent cyberattack help pipeline customers communicate their needs with operators via a computer-to-computer exchange of documents, such as contracts and invoices.'[103]

'ESG's platforms are used "all over the country" for power transactions, Harris said. "Nobody who is using the pricing platform has been able to use it to price since last Thursday. There are going to be estimated bills going out for some of the largest companies." Absent the demand models from Energy Services, retail power providers could also come up short (or long) on power supplies for their customers and may resort to buying and selling in spot markets to re-balance. That could lead to big swings in wholesale prices if Energy Services's system remains down for weeks, Harris said. . . Texas electricity retailers "have been providing manual work-arounds while they await ESG's return to service".[104] This hobbled the operations of at least four natural gas companies[105] with five pipeline operators saying their third-party electronic communications systems were shut down due to hacking[106].

'Though the cyberattack didn't disrupt the supply of gas to U.S. homes and businesses, it underscores that energy companies from power providers to pipeline operators and oil drillers are increasingly vulnerable to electronic sabotage. It also showed how even a minor attack can have ripple effects, forcing utilities to warn of billing delays and making it more difficult for analysts and traders to predict a key government report on gas stockpiles.'[107]

Steve Grobman, chief technology officer at cybersecurity company McAfee Security noted that 'ESG may not even have been the target. . . Instead, the attackers' ultimate goal may have been to find ways to breach ESG's clients. "The level of robustness in the security systems of oil and gas companies makes them difficult targets," Grobman said in an interview on Wednesday. "Going after softer targets such as electronic communications companies is much easier to execute."'[108] This is why it is important that the level of security of electronic transactions for critical infrastructure such as pipelines and electricity grids is high enough and not just left to the private sector which as ESG has shown can choose a level of security that is too weak, given the externalities (see above).

Regulations addressing pipeline security

Some countries have decided that voluntary security standards in the pipeline sector are insufficient and instead have mandated security through regulations. For example 'In 2010 the National Energy Board of Canada mandated security regulations for jurisdictional Canadian petroleum and natural gas pipelines, some of which are cross-border pipelines serving export markets in the United States. Many companies operate pipelines in both countries. In announcing these new regulations, the board stated that it had considered adopting the existing cybersecurity standards "as guidance" rather than an enforceable standard, but "taking into consideration the critical importance of energy infrastructure protection," the board decided to adopt the Standard into the regulations.'[109]

The USA's CRS notes that 'Canada's choice to regulate pipeline security may raise questions as to why the United States has not.'[110]

Regulators' concerns

While the USA still has voluntary/self-regulation of cybersecurity of pipelines, there have been increasing calls for mandatory regulation (including since the ESG attack). For example, the White House, Congressional representatives and regulators have all expressed concern at these cybersecurity risks and proposed mandatory regulations to address them. For example:

- 'An April 2011 White House proposal and the Cybersecurity Act of 2012 (S. 2105) both would mandate cybersecurity regulations for privately owned critical infrastructures sectors like pipelines.'[111]
- In response to the hacking of ESG:
    - '"These attacks are a wake-up call that addressing our aging energy infrastructure needs to be a priority," Congressman Robert Latta, a Republican from Ohio who serves on the House Committee on Energy and Commerce, said in an emailed statement on April 5. "Bad actors are looking at any way to weaken the American energy sector."'[112]
    - Representative James Langevin, co-Chairman of the bipartisan Congressional Cybersecurity Caucus said 'While we continue to learn more about the cyber incidents affecting pipeline business systems including those at Energy Transfer Partners, it should be abundantly clear by now that every business faces cybersecurity risk'.[113]
- In June 2018, two US regulators (one Republican and one Democrat[114]) called for the statutory authority, resources and commitment to implement mandatory standards to address pipeline security.[115]

Insecure stock trading platforms

A security consultant found nearly all of the 40 major online stock trading platforms he investigated had some form of vulnerability.[116] For example:

- 64% of the desktop applications Hernández examined transmitted at least some data eg passwords, balances, portfolios, and personal information unencrypted,
- Most of the web platforms examined did not enable two-factor authentication by default

Requiring these platforms (which are used for huge amounts of money) to use encryption to transmit sensitive personal information, or mandatory two-factor authentication (as some governments do for online banking, see above) would not be allowed under the ecommerce proposals above (unless it is the one category permitted as an exception in some ecommerce proposals).

Facebook sending data to app creators unencrypted

For years, user data was being sent unencrypted by Facebook to the person or company which created the app: 'every time the user loads the app, Facebook sends it a payload of basic user data to facilitate the app's operation (additional data can be requested separately when needed). For years, these transmissions were even conducted unencrypted, until Facebook required apps to communicate with its service over a secure connection.'[117] Presumably Facebook and the app creator would be 'parties to an electronic transaction', so if a government wanted sensitive user personal information (eg health or identifying information) to be sent encrypted, requiring this would not be permitted by the ecommerce proposals above (unless it is the one category permitted as an exception in some ecommerce proposals).

Third-party analytics services using unencrypted http

'Session replay scripts are provided by third-party analytics services that are designed to help site operators better understand how visitors interact with their Web properties and identify specific pages that are confusing or broken. As their name implies, the scripts allow the operators to re-enact individual browsing sessions. Each click, input, and scroll can be recorded and later played back. . .

"Collection of page content by third-party replay scripts may cause sensitive information, such as medical conditions, credit card details, and other personal information displayed on a page, to leak to the third-party as part of the recording," Steven Englehardt, a PhD candidate at Princeton University,

wrote. "This may expose users to identity theft, online scams, and other unwanted behavior. The same is true for the collection of user inputs during checkout and registration processes."

Englehardt installed replay scripts from six of the most widely used services and found they all exposed visitors' private moments to varying degrees. During the process of creating an account, for instance, the scripts logged at least partial input typed into various fields. Scripts from FullStory, Hotjar, Yandex, and Smartlook were the most intrusive because, by default, they recorded all input typed into fields for names, e-mail addresses, phone numbers, addresses, Social Security numbers, and dates of birth. . .

Another example: the account page for clothing store Bonobos leaked full credit card details—character by character as they were typed—to FullStory. Adding insult to injury, Yandex, Hotjar, and Smartlook all offer dashboards that use unencrypted HTTP when subscribing publishers replay visitor sessions, even when the original sessions were protected by HTTPS.'[118]

Presumably the use of third-party analytics services by a company such as Walgreens pharmacy would be 'parties to an electronic transaction' and since it was being sent unencrypted (see above), if a government imposed encryption requirements for transmission of personal information about its residents (as Massachusetts requires), or a social security number (as California and Minnesota require) entered onto the Walgreens website, this would be illegal government interference under the ecommerce proposals above (unless it is the one category permitted as an exception in some ecommerce proposals or one of the difficult to use exceptions applies, see below).

Credit reporting company (Equifax)

'On September 7, 2017, the massive credit reporting company Equifax publicly revealed a breach of the company's computer systems – described as "one of the largest risks to personally sensitive information in recent years" – that exposed data from over 145 million Americans to criminal hackers. The company indicated that a vast trove of sensitive data – including social security numbers, credit card numbers, passport numbers, and driver's license numbers – may have been compromised. The incident was the fifth recent data breach of Equifax or its subsidiaries that endangered American's personal information.'[119]

This was not the only time Equifax had cybersecurity problems. For example during the same period:

- 'Equifax reported in February 2017 that a technical issue "compromised credit information of some consumers who used identity-theft protection services from a customer."'[120]
- 'By July, 14 public-facing websites run by Equifax had expired certificates, errors in the chain of certificates, or other web-security issues.'[121]
- To deal with the breach, 'Equifax set up a website, EquifaxSecurity2017.com, and instructed consumers to visit to determine whether their data were compromised' however 'according to cybersecurity experts consulted by Senator Warren's staff, EquifaxSecurity2017.com had major security vulnerabilities: . . that the site's design and web address made it easy for others to impersonate and collect consumers' information. To demonstrate this, a cybersecurity expert created a website with a nearly identical web address – www.securityequifax2017.com – which looked so similar to the actual website's link that Equifax directed consumers to the fake site multiple times. In addition, experts consulted by Senator Warren's staff identified numerous other technical flaws in the website design. They reported that the website was set up to run on a stock installation of Wordpress, which didn't include the necessary security features to protect the sensitive information consumers submitted, and that the website's Transport Layer Security certificate also did not perform proper revocation checks, which would have ensured that it was establishing a secure connection and protecting a user's data. And then, on October 12, Equifax was forced to take down a web-page where people could learn how to get a free credit report when a security analyst reported that the site's visitors were targeted by malicious pop-up ads. After failing to protect consumer data, Equifax subsequently set up a website that put their customers in even greater danger.'[122]

Equifax 'has "data on approaching a billion people," and "manage[s] massive amounts of very unique data,"' but their inadequate cybersecurity 'put millions at risk of identity theft for the rest of their lives.'[123] 'Equifax prioritized growth and profits – but did not appear to prioritize cybersecurity.'[124] The desire of private companies to maximise profits and therefore behave in ways that can harm consumers can also be seen in how Equifax handled this breach:[125]

- it did not make the breach public for more than a month (so hackers could have used the stolen credit card data etc for a month),
- it did not disclose the fact that passport numbers had also been accessed,
- four months after the breach it had only notified (by phone or in writing) 2.5 million of the 145 million consumers affected (the rest had to know to go to the Equifax website to find out for themselves),
- It charged consumers to freeze their credit to deal with the problem of potential identity theft that Equifax's negligence had created (until there was a public outcry) and profited in other ways outlined in the report from the breach

While the ecommerce proposals above leave it to the 'parties' to an electronic transaction to decide how secure it should be, in reality, consumers have little power to influence how securely private companies such as banks and credit reporting agencies handle their data. For example 'Consumer concerns about the Equifax breach were particularly stark because the company – along with the two other large credit reporting agencies, Experian and TransUnion – occupy a unique place in the financial world: they obtain and use massive amounts of data on millions of consumers, but consumers have little to no power over how this data is collected, how it is used, or how it is kept safe.' [126]

US Senator Elizabeth Warren set up the Consumer Financial Protection Bureau, was Chair of the Congressional Oversight Panel for the Troubled Asset Relief Program (TARP) in the aftermath of the 2008 financial crisis and was a Harvard Law School Professor.[127] Senator Warren wrote a February 2018 report on the Equifax breach which found that:[128]

- 'Sensitive information belonging to over 145 million Americans was exposed as a result of the breach – one of the largest and most significant data security lapses in history.'
- 'Equifax Set up a Flawed System to Prevent and Mitigate Data Security Problems. The breach was made possible because Equifax adopted weak cybersecurity measures that did not adequately protect consumer data. The company failed to prioritize cybersecurity and failed to follow basic procedures that would have prevented or mitigated the impact of the breach. For example, Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability – but then failed to confirm that the fixes were made. Subsequent scans only evaluated part of Equifax's system and failed to identify that the Apache Struts vulnerability had not been remediated.
- Equifax Ignored Numerous Warnings of Risks to Sensitive Data. Equifax had ample warning of weaknesses and risks to its systems. Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems. The company had been subject to several smaller breaches in the years prior to the massive 2017 breach, and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed – or was unable to effectively heed – these warnings.'
- 'the breach was made possible because Equifax adopted weak cybersecurity measures that failed to protect consumer data – a symptom of what appeared to be the low priority afforded cybersecurity by company leaders. The CEO at the time of the breach, Richard Smith, testified that despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity – approximately 3 percent of its operating revenue over the last three years. In contrast, Equifax paid nearly twice as much in dividends to shareholders. Cybersecurity experts

consulted by Senator Warren staff indicated that a large company that holds sensitive data, such as Equifax, should have multiple layers of cybersecurity. . . Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures.'

- The report details various weaknesses in Equifax's cybersecurity
- 'Equifax and other credit reporting agencies have taken advantage of consumers for years, collecting their data without permission and turning a huge profit while failing to adequately protect that data. **These practices won't change without federal legislation that forces Equifax and its peers to put appropriate emphasis on protecting consumer data.'**
- 'Federal Legislation is Necessary to Prevent and Respond to Future Breaches. Equifax and other credit reporting agencies collect consumer data without permission, and consumers have no way to prevent their data from being collected and held by the company – which was more focused on its own profits and growth than on protecting the sensitive personal information of millions of consumers. This breach and the response by Equifax illustrate the need for federal legislation that (1) establishes appropriate fines for credit reporting agencies that allow serious cybersecurity breaches on their watches; and (2) **empowers the Federal Trade Commission to establish basic standards to ensure that credit reporting agencies are adequately protecting consumer data**.'
- **'Congress should empower the FTC to establish requirements for fundamental cybersecurity measures at credit reporting agencies.'**
- 'There have been breaches at all three credit reporting agencies in the last several years, and hundreds of millions of consumers have been impacted. When credit reporting agencies collect personal data without consumer permission, the burden should be on them to protect that data. If they fail to protect that data, they should be punished. Consumer lawsuits do not provide adequate deterrence for companies like Equifax. While the average consumer recovers less than $2 through civil lawsuits in response to data breaches, Equifax is actually set to make money off their recent breach. **If our laws don't punish companies like Equifax for their failure to protect sensitive consumer data, these companies will continue to adopt sub-standard security measures**.'

Health data

'Cybersecurity attacks have the potential to yield disastrous results for healthcare providers and society as a whole. It is imperative healthcare providers acknowledge the need to address cybersecurity concerns and act accordingly. . . medical information is indeed valuable, especially when sold on the black market or used in connection with other unlawful or illicit activities.'[129]

'Companies are increasingly opening their networks to business partners, third-party contractors (including cloud application and storage providers) and even to their customers. To fully address your risk of data theft, you must understand the web of connections to and from your sensitive data. . . What data lives on their infrastructure and what security exists to protect data in transit and at rest?'[130] These third-party contractors may then transfer the sensitive health data to others, so 'BucklySandler Managing Director Rena Mears said. "Companies must understand managing data risk is not merely a compliance and contract issue but a fundamental strategic challenge in which personal data, intellectual property and transactional records must be protected from third, **fourth and nth-party risk.**"'[131]

To do this effectively, companies should ask potential partners specific data encryption questions organizations 'instead of just accepting the generic encryption platitudes.'[132] These could include questions about:

- 'Encryption status of data in transit from database to app server
- Encryption status of data in transit from app server to proxy server (HTTP server)

- Encryption status of data in transit from proxy server to end user's client
- Encryption status of data in transit from API servers to end user's clients (iOS, Android, etc.)
- Encryption status of server to server file transfers'[133]

However a survey of companies (generally, not healthcare companies alone) found:[134]

- 'Half of respondents (49%) confirm their organization experienced a data breach caused by one of their vendors'
- '73% of respondents see the number of cybersecurity incidents involving vendors increasing;'
- '58% of respondents say they are not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach;'

Furthermore, 'Researchers found that a major difficulty is detecting and mitigating risks related to business associates because organizations do not have the resources or procedures to check vendor security measures.'[135]

The USA's Health Insurance Portability and Accountability Act (HIPAA) does not require that patients' data must be encrypted in transit (it is merely addressable[y])[136]. When US hospitals and doctors etc were surveyed, 'only 68.1% of acute providers and less than half (48.4%) of non-acute providers are encrypting data in transit. This means that the providers that are not encrypting data are sending protected health information and other data in the clear, leaving such data susceptible to being breached by eavesdropping, packet sniffing, or other means. Additionally, the lack of encryption means that data may be tampered in transit—thus, there is little assurance that the sender's data has fidelity with the receiver's data. Tampering with such information may have an adverse effect on clinical operations, administrative operations, and/or patient care.'[137]

For example an email containing sensitive data (name, date of birth, gender, and Medicare Beneficiary information) covered by HIPAA was emailed to another medical group without encryption to the relevant level.[138]

Therefore when it is left to the private sector to choose the level of security of electronic transactions, despite the frequency of patient data breaches and the potentially severe health and privacy etc consequences of such breaches, healthcare providers often do not encrypt data in transit. In addition, despite the frequency of data breaches caused by their vendors, companies do not have the capacity to check their vendors' cybersecurity. Governments may therefore need to regulate this highly sensitive sector, however if the ecommerce proposals banning (except perhaps for one category of transactions) the ability to set authentication methods are accepted, this may not be possible. See below for discussion of the adequacy of the usual health exception in trade agreements.

US regulators already realise existing regulations are insufficient

The US government's Federal Trade Commission (FTC) has stated that "additional tools are necessary" to establish basic cybersecurity requirements and monitor companies' adherence to those standards.[139]

The US government's Consumer Financial Protection Bureau (CFPB) claims that '"federal laws that are applicable to data security have not kept pace with technological and cybersecurity developments…it is imperative for Congress to take steps to ensure that the regulatory framework is adequate to meet" the challenges posed by cybersecurity threats'.[140]

The Trump Administration 'is also participating in discussions Congress is having about the requirements of protecting personal data'.[141]

[y] Which means that the company can choose not to implement an addressable specification based on its assessment, but 'it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure', https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf.

Some implications when combined with other ecommerce etc proposals

When considering the potential implications of agreeing to the above eauthentication proposals, it is important to consider the combined effect with other ecommerce etc rules being proposed in these trade negotiations. For example, other provisions in the TPP/proposed in the WTO ecommerce discussions or in other trade agreements include:

- Allowing cross-border data flows (including restrictions on requiring the data to be stored locally). This usually requires a country to allow even its sensitive data (eg health/financial/tax records) to be transferred to any country in the world (which may have insufficient privacy exceptions allowing the data to be sold to advertisers/banks/insurance companies who can then deny bank loans/insurance etc).[z] Combining this with the proposed eauthentication rules above would mean that governments cannot require this sensitive data be encrypted while it is in transit to these other countries, nor can they require it to be encrypted while stored in these other countries etc. This would leave the sensitive data (including credit card details etc) vulnerable to being stolen in the other countries.
- Restrictions on requiring companies to have a local presence (such as a branch/office/subsidiary etc).[aa] If Uber does not have an office in the country concerned, it is very difficult for that country to enforce their laws (including on eauthentication eg to require encryption) on that company (eg to sue them in domestic courts for failure to comply or to enforce a fine on them for not complying with the required level of security in electronic transactions).

As one law professor noted, 'Domestic consumer protections and privacy laws may become impotent if offshore financial firms are not required to have any local presence. When financial data is held 'in the cloud', people's personal and commercial information is subject to the privacy and consumer protection regime of the country that hosts the server – especially problematic when the host is the US.'[142] Therefore it is important to consider the implications for a country's laws/policies etc of the combined effect of the proposed rules, not just the eauthentication proposal in isolation.

Effectiveness of exceptions

Health/environment exception

It is not clear whether the health, environment and privacy exceptions in the WTO's services rules[143] will apply to the ecommerce rules proposed at the WTO. In the TPP, the health, environment and privacy exceptions in the WTO's services rules applied to the TPP ecommerce chapter, so this may also occur in other FTAs.

However, this WTO general exception for health, environment and privacy is difficult to use because of all the tests which have to be passed to use it. By 2015, countries had tried to use this exception (and the equivalent for goods[144]) at the WTO 44 times and only succeeded once, for asbestos[145].

Privacy exception

Furthermore, the privacy exception at the WTO[146] is even more difficult to use because it has an additional phrase which many legal experts believe makes it self-cancelling: it can only be used for laws/regulations which already comply with the Agreement (in which case the exception is not needed). So if this is copied into an FTA which has the eauthentication provisions above, it still requires compliance with the eauthentication provisions above, so it is unlikely that it could be used as an effective exception.

---

[z] Eg see Briefing 3 at https://www.twn.my/briefings_MC11.htm.

[aa] While this has been proposed at the WTO in the name of ecommerce, eg see JOB/GC/97/Rev.3 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx, in FTAs this can often be in the services chapter, eg Art 10.6 TPP, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/

Prudential defence

The WTO does have a prudential defence which is also basically copied into some FTAs such as the TPP[147]. Even if the concerns above (eg re theft of credit card details/identity theft etc) are 'prudential' reasons for regulations (prudential is usually not defined in the text, but it may be clarified in the negotiating history of the trade treaty), this prudential defence also has a phrase which many experts think makes it self-cancelling[148] ('Where such measures do not conform with the provisions of the Agreement, they shall not be used as a means of avoiding the Member's commitments or obligations under the Agreement'[149]). Therefore governments such as the European Union (EU) and USA have not relied on it in some of their FTAs. Eg:

- in the TPP, US financial regulators did not appear to think that this prudential defence would be enough to allow them to require financial data to be stored locally so they could access it in time in a financial crisis[150] (eg to unwind positions held by Lehman Brothers when it collapsed and the data was held in Hong Kong but the IT systems had been switched off and the IT staff left[151]), even though it applies to the ecommerce chapter, so they insisted on explicitly excluding financial data from the prohibition on requiring data to be stored locally in the TPP's ecommerce chapter[bb].
- In some EUFTAs eg the Canada-EU FTA (CETA)[152] and Article 104 of the EU-CARIFORUM EPA[153] the second self-cancelling sentence of the GATS prudential defence has been deleted because presumably those governments thought it made the exception ineffective.

Other exceptions

There are no exceptions in the WTO rules (or in the FTAs which have been checked by this author) for consumer rights more broadly or for efficiency/cost-reductions etc which are some of the reasons that governments have imposed standards for electronic transactions above.

Conclusion

A few hours of searching online by a researcher who is not a cybersecurity expert already found:

1) private companies having insecure electronic transactions (which are or may need to be regulated) in a variety of situations including:

a) backing up their data to the cloud,

b) childcare centre webcam for parents to check on their children

c) online banking

d) apps

e) third-party analytic services etc

2) government set standards for electronic transactions in:

a) Online banking

b) Credit card use

c) Social security number transmission and use on a website

d) Transfer of personal information[cc] electronically

[bb] Art 14.1 TPP: definition of 'covered person' 'does not include a "financial institution" or a "cross-border financial service supplier of a Party"

[cc] Defined to be a human being's first name/'first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

(b) Social security number.

(b) Driver's license number, driver authorization card number or identification card number.

(c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

e) Healthcare

f) Legal settlements (eg by national consumer protection agencies or subnational attorneys general) that require companies (whose inadequate cybersecurity led to data breaches) to increase their cybersecurity, eg by encrypting data in transit or using multifactor authentication

Governments are setting these standards to prevent identity theft or monetary theft, to protect privacy, promote efficiency and lower cost etc. Governments have intervened with regulation in these areas because leaving it to the private sector has been problematic (eg the private sector has not voluntarily adopted secure enough standards, or has not agreed a common system of electronic transactions that increases efficiency and reduces costs etc). One of the reasons that governments have intervened is because of the market failures due to: i) externalities associated with insufficient security: the costs of a security breach are borne largely by entities other than the company that suffered the breach because of inadequate security; ii) information asymmetry: consumers have no way of telling whether a company is providing adequate security.[154]

It is unclear what the perceived problem is which prompted these ecommerce proposals and whether benefits are so great from restricting/banning the government's ability to set standards in these electronic transactions that they outweigh the costs of having to cancel these existing laws and restrict future policy space in a field of fast changing technology.

Even when an exception is allowed, it seems to be limited to 'a particular category of transactions' (TPP ecommerce chapter and the EU's 2017 esignature/eauthentication proposal at the WTO). This appears to mean that governments agreeing to such a provision would have to choose one of the areas above where it could set standards (this does not even consider future areas which may need regulation eg genetic information (see below)). Furthermore, the EU's FTA and 2018 WTO ecommerce proposals allow no exceptions at all, the private sector must always be allowed to set as low standards as it wants (eg to save on costs and thus to make more profits).

As noted above, relying on the usual general exceptions for health/privacy/prudential reasons are unlikely to be sufficient.

As can be seen above, leaving it to the 'parties to an electronic transaction' to decide how secure it should be can already be problematic in a business-to-business transaction where one or both companies want to cut costs. It is even worse in when one of the 'parties' to the transaction is a consumer (eg in online banking, credit reporting, DNA testing, online shopping etc) who has little or no power to determine how secure the transaction should be. The situations above are already real world problems from leaving it to companies to decide how secure an electronic transaction would be.

The examples above are just some of those which happen to have been seen in recent news reports. There have been many other reports of the lack of secure transmission of sensitive personal information by private companies such as webcams monitoring a childcare centre[dd] and dating apps.[ee]

(d) A medical identification number or a health insurance identification number.

(e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.'

[dd] The childcare centre allowed parents of the children enrolled to check on their children in the childcare centre via a webcam. However this did not use https, so the data was not encrypted. The Office of the Privacy Commissioner of Canada recommended that https be used for this webcam, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008/. It is unclear if this kind of situation would be covered by 'parties to an electronic transaction' (where government intervention is restricted in the ecommerce proposals), see above.

[ee] Eg the world's most popular dating app did not use https for its photos, swipes or matches so they are unencrypted and 'Just by being on the same Wi-Fi network as any user of Tinder's iOS or Android app, the researchers could see any photo the user did, or even inject their own images into his or her photo stream. And while other data in Tinder's apps are HTTPS-encrypted, Checkmarx found that they still leaked enough information to tell encrypted commands apart, allowing a hacker on the same network to watch every swipe left,

There are likely to be many more circumstances where leaving it to the private sector to determine the level of security may result in a lower level of security than is required for consumer protection, privacy etc as companies try to minimise costs.

The Equifax example above shows that even if there is no current legislation requiring such data to be held, transmitted, processed etc more securely, there is already a need for such legislation according to a US Senator widely acknowledged as an expert in consumer financial protection.

Furthermore, as electronic transactions become more widespread, even more sensitive personal data (eg health, financial records etc) are likely to be transmitted electronically with the increased risks that involves.

The laws requiring a certain level of security in electronic transactions between private parties described above are just those that could be found with little effort. A systematic search of all measures (eg laws, regulations, directives, circulars etc), at all levels of government, in all sectors, government ministries and regulators is likely to find many other measures requiring a certain level of security in electronic transactions. As noted above, national or subnational laws already require electronic transactions to have a certain level of security for consumer protection etc reasons. Under the TPP and some proposed WTO eauthentication provisions, these laws can only be kept for one category of transactions at the most. Under the EU's FTA proposals, all of these laws would have to be deleted since the EU's FTA proposals have no exceptions.

Given the diversity of the sectors affected and variety of ministries already regulating/ planning to regulate electronic transactions (from financial regulation, consumer protection, law enforcement to health etc) at various levels of government, it is important to consult all relevant ministries and levels of government as well as affected economic and social sectors before deciding whether to agree to this kind of ecommerce proposal. For example small shops and restaurants may not want the dominant credit card companies to have the right to continue their current privatised rules locked in.

As the Minnesota government report on data privacy noted in a section titled Legal Landscape Unpredictable: 'It is impossible to predict how the legal landscape relative to data privacy and security will look in the next few months or years to come . . . Federal and state lawmakers continue to grapple with ways to strike a balance between new technology, the free flow of information that has become ubiquitous to e-commerce, the proliferation of social media, and the protection of personal information.'[155] The same report listed 10 federal bills in the USA as just some of those proposing increased data privacy protection in the US Congress as legislators respond to the data breaches.

If even developed country governments are having difficulty keeping up with how quickly technology is evolving, it is even more difficult for developing countries and least developed countries (LDCs) to predict what sectors will have electronic transactions in the future and where governments may need to regulate. When even domestic regulations have trouble keeping up with the speed of technological change, locking in deregulation/laissez faire corporate self-regulation in an international treaty (which is even slower to amend if it turns out to be problematic in a time of rapid technological change) risks being out of date by the time the trade agreement comes into force.

It is surprising that at a time when more and more examples of insufficient cybersecurity by private companies are being found, and developed, developing and least developed governments are planning new regulations to deal with these, that trade negotiations are contemplating (total) deregulation of this issue, leaving it to private companies to set the standards when many such companies have chosen inadequate levels of cybersecurity (which cause problems for consumers etc) when left to choose the level of security themselves.

---

swipe right, or match on the target's phone nearly as easily as if they were looking over the target's shoulder. The researchers suggest that lack of protection could enable anything from simple voyeuristic nosiness to blackmail schemes', https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/

Annex: potential future cybersecurity problems

Unauthorised access to/use of genetic information/DNA

DNA and genetic information needs to be secure. It can reveal information about your health, personality, family history etc[156] and 'researchers have already shown that it is possible to identify some people based on anonymous genetic data. In 2013, an MIT professor published a study in which he successfully identified people and their relatives based on "anonymous" genetic data in a research study, along with only their age and a state.'[157] Even when some of the genome is left out (eg James Watson did not publish the part of his genome indicating whether he is more likely to develop Alzheimer's), that can be predicted based on surrounding DNA.[158]

a. US Senator Schumer put out a press release in November 2017 about at-home DNA test kits which 'require a cheek swab or the collection of saliva, which is then sent away for genetic-testing

   i. . . . Over the past several years, DNA testing kits have become more and more popular. According to media reports, the DNA testing market was worth approximately $70 million in 2015 and is expected to rise to $340 million by 2022. . .

   ii. Many consumers purchase DNA test kits, from companies like MyHeritage, Ancestry and others to learn more about their genetics and ancestry, however, many don't realize that their sensitive information may end up in the hands of many other third party companies. . .

   iii. Schumer points out that each company has its own variation of a privacy policy and Terms of Service and that many companies may be selling the genetic data they've gathered to third parties. Schumer today said that it is clear more must be done to protect consumer privacy when it comes to these at-home DNA testing kits. . .

   iv. When it comes to protecting consumers' privacy from at-home DNA test kit services, the federal government is behind. Besides, putting your most personal genetic information in the hands of third parties for their exclusive use raises a lot of concerns, from the potential for discrimination by employers all the way to health insurance. . . That's why I am asking the Federal Trade Commission to take a serious look at this relatively new kind of service and ensure that these companies have clear, fair privacy policies and standards for all kinds of at-home DNA test kits.'[159]

b. Senator Schumer noted that 'Here's what many consumers don't realize, that their sensitive information can end up in the hands of unknown third-party companies," he said. "There are no prohibitions, and many companies say that they can still sell your information to other companies." "Now, this is sensitive information, and what those companies can do with all that data, our sensitive and deepest information, your genetics, is not clear and in some cases not fair and not right," he added.' He concluded that the companies 'are brand new, and they need safeguards.'[160]

c. A consumer protection lawyer noted that when you send your sample to a DNA testing companies 'It's basically like you have no privacy, they're taking it all'[161]. The DNA testing companies provide your genetic data to other companies and it is not clear 'who all of those third parties are and what kinds of rules the companies put in place to prevent those third parties from abusing the access to genetic information.'[162]

d. Many others have expressed concern about the lack of privacy and security protections in the DNA kit market including a former US Food and Drug Administration Associate Commissioner Peter Pitts: 'I would never sign away the rights to my genes. . . You shouldn't either.'[163] 'The other thing that's clear is that genetic testing companies are definitely selling information to third parties for medical research in order to make

money. “Using this information for clinical trials is a good thing,” said Pitts. “But do you want some third party organization selling that information to pharmaceutical companies? How secure is your data in that third party environment? You don’t know.”’[164]

Failure to protect genetic information adequately has already had consequences

While the USA has the Genetic Information Non-Discrimination Act (GINA) which is supposed to prevent ‘health insurers and workplaces from discriminating based on your genetic information, gaps in the law mean that life, long-term care, or disability insurance providers as well as the military can still make decisions based on findings from your DNA.“GINA actually provides very little protection,” said Ellen Wright Clayton, a lawyer and professor of health policy at Vanderbilt University.’[165]

‘Since 2008, with the passing of the Genetic Information Nondiscrimination Act (GINA), the federal government has barred health insurance companies from denying coverage to those with a gene mutation. But the law does not apply to life insurance companies, long-term care, or disability insurance. These companies can ask about health, family history of disease, or genetic information, and reject those that are deemed too risky.’[166]

‘“At the beginning of this decade-long saga, the bill [GINA] included every type of insurance,” says Terry. But early proponents of the bill threatened to drop their support if it included disability, life insurance, and long-term care,’[167] so they were excluded from GINA.

The insurance industry ;makes the case that the business model would crumble if companies are forced to accept those with a high risk of cancer and various genetic diseases into the pool.

There is some truth to this argument. Brigham and Women’s Hospital’s Dr. Green studied the behavior of those who learned via a genetic test that they were predisposed to Alzheimer’s Disease. These patients were five times as likely to buy long-term care insurance than those in a control group.

And rather uniquely, health insurers are able to offset their risk by taking in monthly premiums from young and healthy Americans (the Affordable Care Act’s “Individual Mandate” requires that many people get health insurance or face a penalty). By contrast, a decision to purchase life insurance or long-term care insurance is optional. Those who apply for policies might have reason to believe that they need additional protections.’[168]

‘California passed a bill called CalGINA that not only prohibits genetic discrimination in employment and health insurance, but also in housing, education, mortgage lending, and elections. Oregon and Vermont also have broad regulations prohibiting the use of genetic information in life, long-term care, and disability insurance.’[169]

A patient has already been denied life insurance because she had the BRCA1 gene which is associated with increased risk of breast and ovarian cancer and a father at increased risk of prostate cancer refused to test for it (even though it would help prolong his life) because he could be denied life insurance.[170]

‘GINA’s loophole hasn’t just caught the attention of patients’ rights groups. Medical researchers are also growing increasingly concerned that it will set back their clinical trials and studies.

Green directs a randomized trial to study gene sequencing in adults called the MedSeq project, which relies on patients agreeing to store their genome sequencing data in their medical record. As he recently reported in the New England Journal of Medicine, 25% of patients who declined to participate in the study cited fear of discrimination from life insurance companies as their primary reason.

Green expects that more patients will bow out of clinical studies and genetic tests as they become aware of the downsides.

“Before GINA passed, a lot of people were afraid that this new era of genetic testing wouldn’t include proper protections for patients,” says Green. “But there’s still reason to be afraid that companies will discriminate against whole families.”’[171] When doing a study sequencing the genome of babies, Green ‘got a 10 percent recruitment rate—to get 300 families they had to ask 3,000. “There are a lot of

reasons," says Green, "but about the third most common was concerns about privacy and discrimination."'[172]

Consumer genetic testing firms are not usually bound by the USA's regulations on health data privacy

While the USA has the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of health data, 'because consumer genetic testing firms are not typically bound by HIPAA, the flow of your data is basically unregulated, said Bob Gellman, a privacy and security consultant. That means any authorized recipient of your information could easily pass it along to someone else. "Any data anywhere can be hacked in one way or another. That just happens today," said Gellman. "The more people have the same data, the more there's risk to the data. That's just a given."'[173]

Genetic data could be stolen by hackers

'genetic data is much more sensitive, and people (rightly) worry that it might be used against them by insurers, or even stolen by hackers.'[174] Microsoft's head of cryptography research who focuses on DNA encryption noted that "If we don't think about it now, in five to 10 years a lot people's genomic information will be used in ways they did not intend".[175]

Common DNA-processing programs are extremely vulnerable to hackers

'common, open-source DNA-processing programs are super vulnerable to hackers'.[176] 'Researchers looked at commonly used, open-source versions of those programs. Many, they found, were written in programming languages known for having security issues. Some also contained specific vulnerabilities and security problems. "This basic security analysis implies that the security of the sequencing data processing pipeline is not sufficient if or when attackers target," they wrote.'[177]

The insecurity of these programs have implications for criminal justice: 'Greg Hampikian, a professor of biology and criminal justice at Boise State said the more immediate vulnerabilities the researchers highlighted are concerning. "If you could break into a crime lab you could alter data, but if you can break into the crime lab's data, you have a much more efficient route. And if the data is altered, that's what will be used to testify in court," he said. "We've had accidents where tubes have been swapped. If you could maliciously alter or erase that's obviously a big problem."'[178]

An academic expert commenting on the lack of security of consumer DNA testing companies noted that '"With 23andMe and Ancestry you're signing over your DNA to them, and how are they handling DNA security? There that data is linked to your name," he said. Because it's unclear how that data is secured and used, he told Gizmodo, he even recommends that his students steer clear of consumer DNA tests. "There's nothing more sensitive than someone's DNA," he said.'[179]

More secure ways of handling genetic data are available

More secure ways of handling genetic data are available such as encrypting it.[180].

However when left to decide for themselves, private companies are not choosing to use these more secure methods (presumably because of concerns about cost). Therefore governments may need to regulate to ensure a certain level of security in transmitting, storing, processing etc highly sensitive personal data such as genetic information.

---

[1] https://www.internetsociety.org/globalinternetreport/2016/
[2] Page 98
[3] https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf
[4] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity
[5] https://www.internetsociety.org/globalinternetreport/2016/
[6] See pipeline section below
[7] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

[8] https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/
[9] TN/S/W/64 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx
[10] JOB/GC/188 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx
[11] WT/L/274 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.
[12] WT/MIN(17)/60 from https://www.wto.org/english/thewto_e/minist_e/mc11_e/documents_e.htm
[13] Art 8.77.3 http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684
[14] Art 6.3 of the digital trade chapter http://trade.ec.europa.eu/doclib/press/index.cfm?id=1833
[15] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[16] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[17] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[18] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[19] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[20] https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/
[21] Eg see https://www.entrepreneur.com/article/281633.
[22] See Request Pricing for All HTTP Methods (per 10,000) table at https://aws.amazon.com/cloudfront/pricing/
[23] https://techcrunch.com/2017/10/30/aws-continues-to-rule-the-cloud-infrastructure-market/
[24] https://www.entrepreneur.com/article/281633
[25] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[26] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories
[27] www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
[28] NRS 603A.215.2 https://www.leg.state.nv.us/NRS/NRS-603A.html
[29] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf
[30] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[31] https://oag.ca.gov/idtheft/facts/your-ssn
[32] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[33] https://www.ssa.gov/pubs/EN-05-10064.pdf
[34] https://www.ssa.gov/pubs/EN-05-10064.pdf
[35] https://oag.ca.gov/idtheft/facts/your-ssn
[36] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[37] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[38] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[39] https://oag.ca.gov/idtheft/facts/your-ssn
[40] Eg see https://www.wcpo.com/money/consumer/dont-waste-your-money/what-your-accounts-are-worth-on-the-dark-web
[41] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[42] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[43] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[44] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[45] http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.85.
[46] Minn.Stat §325E.59: Use of Social Security Numbers, https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf written by a law firm, https://mn.gov/deed/newscenter/press-releases/?id=1045-229996
[47] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html
[48] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html
[49] Art 29.1 TPP
[50] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Operating-Rules/OperatingRulesOverview.html

[51] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Operating-Rules/OperatingRulesOverview.html
[52] Art 29.1 TPP
[53] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html
[54] https://www.youtube.com/watch?v=s_1CZYK8qb8
[55] https://www.youtube.com/watch?v=s_1CZYK8qb8
[56] https://www.caqh.org/core/operating-rules-mandate-eft-and-era
[57] Art 29.1 TPP
[58] https://www.theguardian.com/technology/askjack/2017/jun/22/is-it-safer-to-use-an-app-or-a-browser-for-banking
[59] http://www.bbc.com/news/technology-42353478
[60] https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=8207
[61] Section 500.15 https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
[62] Section 500.12 https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
[63] Art 14.6 https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/
[64] https://www.ftc.gov/about-ftc
[65] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf , eg see complaint at https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter, see also https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[66] Complaint at https://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter
[67] Complaint at https://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter
[68] https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx
[69] https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[70] Complaint at https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter
[71] https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[72] NRS 603A.215.1 https://www.leg.state.nv.us/NRS/NRS-603A.html
[73] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[74] https://www.pcisecuritystandards.org/about_us/
[75] https://www.westpac.com.au/docs/pdf/bb/Guide_to_payment_card_indus1.pdf
[76] https://blog.pcisecuritystandards.org/pci-monitor-2-8-2017
[77] https://www.wired.com/2012/01/pci-lawsuit/
[78] https://www.wired.com/2012/01/pci-lawsuit/
[79] https://www.forbes.com/forbes/2010/0628/entrepreneurs-heartland-payment-visa-mastercard-once-hacked.html#10ea72fe6f32
[80] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[81] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[82] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[83] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[84] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[85] https://www.forbes.com/forbes/2010/0628/entrepreneurs-heartland-payment-visa-mastercard-once-hacked.html#10ea72fe6f32
[86] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[87] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[88] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[89] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[90] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-001/
[91] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[92] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[93] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[94] https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy
[95] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf
[96] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[97] https://www.usnews.com/news/best-states/alaska/articles/2018-03-16/trans-alaska-pipeline-fights-22-million-cyberattacks-per-day
[98] https://fas.org/sgp/crs/homesec/R42660.pdf

[99] https://www.usnews.com/news/best-states/alaska/articles/2018-03-16/trans-alaska-pipeline-fights-22-million-cyberattacks-per-day
[100] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[101] http://www.post-gazette.com/powersource/companies/2018/04/02/Cyber-attack-shuts-Energy-Transfer-s-pipeline-data-system-EDI/stories/201804020114
[102] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[103] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[104] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[105] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[106] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[107] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[108] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[109] https://fas.org/sgp/crs/homesec/R42660.pdf, see https://apps.neb-one.gc.ca/REGDOCS/File/Download/614556 for Canadian decision to make it mandatory.
[110] https://fas.org/sgp/crs/homesec/R42660.pdf
[111] https://fas.org/sgp/crs/homesec/R42660.pdf
[112] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[113] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[114] https://www.bloomberg.com/news/articles/2018-06-11/u-s-regulators-urge-better-oversight-for-pipeline-cybersecurity
[115] https://www.axios.com/cybersecurity-threats-to-us-gas-pipelines-call-for-stricter-oversight-09fac6e5-da94-491e-9523-d08ef15237f4.html
[116] https://www.wired.com/story/online-stock-trading-serious-security-holes/, full report at https://ioactive.com/are-you-trading-stocks-securely-exposing-security-flaws-in-trading-technologies/
[117] https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/
[118] https://arstechnica.com/tech-policy/2017/11/an-alarming-number-of-sites-employ-privacy-invading-session-replay-scripts/
[119] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[120] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[121] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[122] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[123] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[124] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[125] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[126] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[127] https://www.warren.senate.gov/about/about-elizabeth
[128] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[129] http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
[130] https://healthitsecurity.com/news/protecting-against-unauthorized-healthcare-data-access
[131] https://healthitsecurity.com/news/are-third-parties-compromising-healthcare-data-security
[132] https://healthitsecurity.com/news/health-data-encryption-questions-to-ask-your-vendors
[133] https://healthitsecurity.com/news/health-data-encryption-questions-to-ask-your-vendors
[134] http://www.marketwired.com/press-release/third-party-vendors-are-key-concern-for-business-data-privacy-survey-finds-2111430.htm
[135] https://healthitsecurity.com/news/are-third-parties-compromising-healthcare-data-security
[136] 45 CFR 164.312e) https://www.law.cornell.edu/cfr/text/45/164.312
[137] http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
[138] https://www.hipaajournal.com/hipaa-breaching-email-exposed-bjc-healthcare-patients-data-8334/.

[139] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[140] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[141] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[142] http://www.thefutureworldofwork.org/stories/uni-global/tisa-foul-play/
[143] Art XIV https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV
[144] https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX
[145] https://www.citizen.org/sites/default/files/general-exception_4.pdf
[146] Art XIVc) https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV
[147] Art 11.11.1 https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/
[148] Eg see http://www.citizen.org/documents/report-prudential-measures.pdf
[149] https://www.wto.org/english/docs_e/legal_e/26-gats_02_e.htm#annfin
[150] http://www.politico.com/tipsheets/morning-trade/2016/02/lew-defends-financial-services-data-carveout-senate-to-vote-on-customs-bill-democrats-weigh-in-on-tpp-212657
[151] http://www2.itif.org/2016-financial-data-trade-deals.pdf?mc_cid=0a36b6ab0c&mc_eid=671b585ee6
[152] http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf (Art 13.16.1 on p103)
[153] (signed in 2008: http://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:289:0003:1955:EN:PDF
[154] See 2016 Global Internet Report of the Internet Society, available at: https://www.internetsociety.org/globalinternetreport/2016/
[155] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf
[156] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[157] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[158] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[159] https://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-popular-at-home-dna-test-kits-are-putting-consumer-privacy-at-great-risk-as-dna-firms-could-sell-your-most-personal-info-and-genetic-data-to-all-comers-senator-pushes-feds-to-investigate_ensure-fair-privacy-standards-for-all-dna-kits
[160] https://www.nbcnews.com/news/us-news/senator-calls-more-scrutiny-home-dna-test-industry-n824031
[161] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[162] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[163] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[164] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[165] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[166] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[167] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[168] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[169] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[170] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[171] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[172] https://www.wired.com/2017/05/house-health-plan-makes-genes-preexisting-condition/
[173] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[174] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[175] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[176] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[177] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[178] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[179] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[180] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/