From:	Andrew Crisp
To:	privacyrfc2018
Subject:	Docket No. 180821780-8780-01
Date:	Tuesday, September 25, 2018 6:09:24 PM

Sorry if this is rambling..... happy to discuss further please email me for more information.

Written comments identified by Docket No. 180821780-8780-01 may be submitted by email to privacyrfc2018@ntia.doc.gov. Comments submitted by email should be machine-readable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Attn: Privacy RFC, Washington, DC 20230
privacyrfc2018@ntia.doc.gov

Data Protection laws should be written for all residents (citizens and non-citizens) for any company organization or entity that obtians/capatures data in any form in the US. Also for non-residents while they are in the US for what ever period of time they are in the US and their data is obtained while they are in the US.
A persons data is there data - a company or organization or entity can not own a persons data nor profit from holding or using the data without the express permission of the owner of the data. (opt-in - not opt-out). If permission is given it should be stated when and how the data can and will be used.

National set to laws not state by state - level playing field for all companines.
Daat protection should be a Bill of Rights for the consumer.

Fines and punishments:
Should be adequite to encourage companies, organizations and entities to do the right thing.
V-tech (leapfrog) data breach of about 650,000 childrens personel data - the fine was $650,000 about $1 per child. A childs personel data is worth more then $1. The potentional cost to the child of a data breach probably can not be calculated.

Toy firm VTech fined over data breach

Toy firm VTech fined over data breach

US regulators say it did a poor job of protecting data it gathered about children and parents.

VTech Electronics Limited

VTech Electronics Limited

The official website of the Federal Trade Commission, protecting America's consumers for over 100 years.

EquiFax -> charging for protection.
The biggest and more important data breach that I have ever heard of.
My data was compremised.
I checked this out and Equifax asked for money to take further action to protect my data.
Who knows who has my data.
The federal government started to investigate then shutdown the investigation.

This looks like the US government favours protecting companies over its citizens.

Equifax -> LexusNexus -> StateFarm
After 25 years of using StateFarm I was told one of my inurance policies woudl be suspended - I had 30 days to find an alternative. This was based upon LexusNexus. State Farm could not tell me why. I wrote to LexusNexus and I'm waiting to hear back. Talking to my state farm agent I got it sorted out. the main breach I know of for my PII is Equifax. How and credit reporting agencies be trusted if they have been breached - companies profit it the information is bad - the information is more likely to be bad if it has been adused. If the companies that perform data collection and review can not be trusted and the government shuts down investigation and the high ranking executives leave a company with heft leaving packages - this is not in the best interest of the people. It is inthe best interest of the companies and executives to maximize returns - are the risks worth while? We need the government to ensure there are adequat concequences so the company and ites executives do right. Jail time / huge fines / no leaving packages - review boards / trails. Its should not just be the company and trhe share holders who are held accountable.

The banks are a great example of the US government letting the bank executive off the hook. Look at Iceland and what happened to their bank executives.

There has to be consequences.

In my work I talk with many Information Technology Admins the Full Time Employees who run IT HW/Software. I have some security features/capabilities that should be in place. I am shocked by the repsonses I get. I belive these responses are due to a lack of direction in the IT organization to take care of security as a every day concern about everything we do. Security seems to be somethign else I have to do - the managers are pushing for results they do not push for results while maintaining security.
A small company in the nucular industry - told me they lock the data center door so data encryption at rest is not a consideration. A small school district removed the data encryption at rest licensing as they did not want to pay about $500 on a $40,000 order.

I have had issuses with the Health Care industry and my data. I had a bill from a Medical Doctor about 3 months after a emergancy room visit. The hospital contract out to the doctors - so the doctors bill

separate from the hospital. I recievved the bill about 3 months after the visting - the bill was not obvious wat it was for - I did not get hte doctors name - I di dnot associate the bill with the visit due to the lapse in time. The bill was not form the hospital but a physicains group. So I called the nuebr on the bill - I was asked to provide identifying information. I would not provide any personel information - I was told that they had my personel information so should just give it. As I wanted to knwo who this organization was I asked fo rthem to prove who they where to may satisfaction - I suggested workign through the hosprial so I can collaberate they where a ligitimate organization and this was not a phising via mail to get my PII. They bulled and threattend to send my account to a collection agent if I did not give them my information over the phone. We badly need rights as consumers. To stop abuse and bulling by organization that use leverage and intimidation to get information.
The issue the way I see it - the admins are not being told that security is there responsibility and what type of security is needed. I have been talking about GDPR and CA AB 375. Still the reation is to wait until they are told they need to do this. They have no direction to do thi. Not saying this is all companies, organizations or entities - it is enough to make me wonder. The cost of the solution is the most important for many many customers not the security. If seniror executives care about security it is not getting down to the full time employees.

Data proection should not just be focused on "IT" companies - any company, organization or entity that hold anyones personel identifiable information is a IT company, organization or entity.

EXAMPLE:
WellsFargo tells customers its has the right to share there data to over 1400 affiliates - 125 out side the US for market purposes. I see this as over reach.

Wells Fargo can customers PII with its affiliates:
For our affiliates to market to you Yes

So who are the affiliates?
Here are the list of affiliates:
WFC-12.31.2014-EX21

WFC-12.31.2014-EX21

The last time I worked on this there was 125 affiliates outside the US.
35 in the Caymon Islands - as Island chain with a population of 60,000 people.
I do not think at least 1 in 1,700 people in the Caymon Islands should have access to my information - just because I used Wells Fargo as a mortgauge processor on a home loan 10 years ago.
I never had a back account / credit card / savings account with Wells Fargo. My home loan was given to Wells Fargo from a different mortgage processor - I do not recall being given a choice.

So while checking out the Cayman Islands - I found that the Cayman Islands is the 8th or so largest holder so US debt. I think this is odd in itself. Make me wonder if the US government runs on laundered money?
That is $3m of US debt per capita of the Cayman Islands.

Then go look at the number of Wells Fargo affiliates in Luxemburg and the US government debt held by Luxemburg - this this is also odd.

Uber - paying off blackmailers to not release information - then the time it takes for companies (not just uber) to reveal they have had data breach.

I wonder about basics - media in the data center going missing and not reported - just stay quiet maybe it will all be forgotten. I think the general believe is to say nothing. I have worked at companies where this has occurred Hard Disk drives where stolen on more than a single occasion. Drive being returned to the manufacture in the mail that goes missing.
A fishing boat company on the bearing sea - they have computers on the ships - when the boat docks if there is a bad hard disk drive to be returned they get a fisherman to get the bad drive and ship it back to there office location.
This week I heard we had a new shipped of $100,000s of equipment disappear in shipping (new so no data).
Encrypting data on the media is easy nowadays - need to make choice - but even in the conversations I have this simple thing is not being considered as important enough.
Those who are not willing to change, Change nothing. We need regulations that have consequences to get people to take this stuff seriously as this will only get worst.

GDPR is a good example of what is needed. I have read through and learned about GDPR as I'm concerned about my personal identifiable information and how I see companies work against consumers best interest.

So what do I think is needed:

A bill of rights for citizens data.

A persons data is the property of the person.

Only use data for the purpose that is was given.

Appropriately protected and used.

Permissions for use and for making money.

Requirements for reporting of breaches.

Rights to be forgotten (where possible / applicable) considering conflicting laws.

Ways for the consumer to report to a centralized body.

I'm sure a lot of companies will complain - if it is a level playing then it is fair to all.
There will always be companies that take advantage - there need to be consequences for taking advantage (crossing the line).

Andrew Crisp
adcrisp@yahoo.com