



INFORMATION INJURY WORKSHOP

Comments for FTC

Abstract

Injury caused by information can affect people, businesses and governments and comes in many forms – financial, psychological, health, reputation, livelihood and freedom.

Bev Corwin, Cindy Cullen, Niloufer Tamboly

Executive Summary

Injury caused by information can affect people, businesses and governments and comes in many forms – financial, psychological, health, reputation, freedom and livelihood to name a few. The cause of the injury can be intentional or unintentional. This paper provides a high-level review of how data used for identity theft, criminal identity theft, business identity theft, medical identity theft can lead to the injury of people and businesses. The data used for these purposes may be obtained via data breaches, deceptive business practices, physical theft or other nefarious activities.

Weaponization of information is becoming more common. On a personal level, information can be weaponized to shame or to humiliate people via cyberbullying, cyber harassment, sexting, etc. The data used in these types of attacks may be real or fabricated.

At the nation state level, information is weaponized for political and nation state activities such as cyber warfare.

It is important when discussing information injury to understand there are protection and prevention mechanisms that can be developed to minimize the impact of injury. Processes to give people and businesses control over their personally identifiable information (PII) are outlined in the frameworks.

Contents

Executive Summary 1
Data Injury 3
Criminal Identity Theft..... 3
Business Identity Theft 4
Reputational 4
Psychological/Emotional..... 4
Shaming 4
Deceptive business practices..... 5
Weaponization of information 5
Impact of Data Injury 5
Medical ID theft 5
Reputational impact 6
Employment/livelihood 6
US States Identity Theft Information and Identity Theft Registry 6
Information Injury Framework 6
Biometric Information Privacy Act..... 7
For Businesses..... 7
Protect What is Collected 7
Internal Documentation/Processes 8
Impact of a Data Breach to the Business..... 8
Mandatory Cyber Insurance 8
Summary 8

DATA INJURY

Personal injury caused by misuse of data is a poorly defined area. The injury can be in many forms. The injury may be from stolen data, mis-use of data, unintended consequences, or intentional use of data that may not be perceived to be injurious by the user. All of these can lead to various forms of personal, corporate and government injury. Personal Injury includes identity theft, criminal identity theft, medical identity theft, and cyber bullying. These can impact a persons' financial, psychology, physical health, legal, reputation, and personal freedoms. Corporate Injury impacts include financial, intellectual property theft, reputation, loss of customers, and potential criminal charges for lack of protection of customer/employee data. Government impacts include compromise of undercover agents (OPM breach), compromise of elections (Russian influence in 2016 presidential election), cyberwar (Stutnex) and escalation to a physical war (TBD).

Data injury via identity theft takes many forms. Personal data injury caused by security incidences include but are not limited to the following:

Identity Theft – creation of identity - driver license, passports in your name can impact:

- Financial
- Credit scores
- Ability to get loans
- Loss of funds from existing accounts (bank, brokerage accounts,....)
- Medical ID theft
- Criminal - Warrants/arrests/tickets -

Criminal Identity Theft

Criminal identity theft is particularly pernicious. Perpetrators use PII to create driver licenses, state identification cards and passports with the stolen identity and their picture. Then use them for nefarious activity. The victim ends up with false mistaken arrest, summons, complaints, felony complaints, indictments or conviction. One typical example, a perpetrator creates the false identity, then presents that identity when given a ticket or arrested. They typically do not show up for court date, the judge then issues a bench warrant for the arrest of the victim of the identity theft. Often the victim becomes aware of the identity theft when they are arrested or terminated from their job because of outstanding warrants or lose custody of their children.

For example, Lance Miller's of Colorado had his wallet stolen. The perpetrator drained Miller's bank account, maxed out his credit cards and was arrested in Miller's name. The real Lance Miller was then arrested and handcuffed in front of his children and taken to jail. Fortunately, the police realized the identity theft and he released.

For Gerber Guzman, the wheels of justice did not turn so quickly. Guzman was falsely arrested twice because of warrants in his name due to identity theft. At one point he spent over two weeks in jail until police eventually checked Guzman's fingerprints. They did not match the warrant.

In 2010, Nicole McCabe, a pregnant 27year old Australian living in Tel Aviv woke up one day to find her identity had been used in the murder of top Hamas leader Mahmoud Al Mabhouh. The

fake passport had all of her identity information. Fortunately, for McCabe the photo in the fake passport was the thief's photo.

Pharmacist Gerald Barnbaum stole Dr. Gerald Barnes identity and practiced medicine even working as a staff physician at a center giving FBI agent medical exams. A type 1 diabetic patient died under his name care. He is presently in Federal Corrections Institute in Loretto, PA.

Gary Wayne Bogle, Washington created a driver license in his brother's name, was arrested and incurred extensive medical dept. A surprising percentage of identity theft is done by family and friends.

Business Identity Theft

Criminal identity theft can also involve the creation of companies such as Limited Liability Corporations with the stolen PII including opening a bank account. The LLC is then used to cash stolen checks,

BJ Services Company is a legitimate company

BJ Services Company was created with identity theft victim's name – Scott Weinbart. With a mail box office, a brokerage account and stolen checks for the real energy company BJ Services the thief cashed over 5 million of dollars in checks and diverted the money off-shore. <https://www.linkedin.com/pulse/criminal-identity-theft-robert-minniti-cpa-cfe-cva-cff-maff-pi/>

Reputational

Ashley Madison breach is an excellent example of how information injury can impact reputations.

- An unknown number of relationships were impacted, spouses, children, work relations and employment
- Additionally, fake data dumps have been developed that impact personal reputation. <https://www.wsj.com/articles/hackers-post-stolen-user-data-from-ashley-madison-breach-1440032355>

Psychological/Emotional

Emotional trauma of not knowing if identity has been stolen leading to anxiety and feelings of helplessness.

Shaming

Carolyn Gregoire argued that "Social media has created an aggressive culture of public shaming in which individuals take it upon themselves to inflict psychological damage" and that more often than not, "the punishment goes beyond the scope of the crime."^[30]

On 24 August 2015, a pastor and professor at the [New Orleans Baptist Theological Seminary](#) committed suicide citing the leak that had occurred six days before.^[37]

Biometrics

The unauthorized use of biometric information including face and body images

Informorphs - use of individuals, chatbots or software to create a digital identity based on a physical facsimile of your face or stolen picture. Infomorph – a virtual body of data that possesses emergent features including personality. This technique was used by Avid Life owner of Ashley Madison to create image of more women available on the site.

Slander-libel – Threats of character assassination/extortion/blackmail in professional environments (workplace, professional associations, etc.), for political or personal gain.

Privacy invasion - Companies such as Shutterbug have the biometric image and tagged name. That can then be leveraged by Shutterbug to tag strangers in the background in photos in public places.

Deceptive business practices

“Ashley Madison's company required the owner of the email account to pay money to delete the profile, preventing people who had accounts set up against their consent (as a prank or mistyped email) from deleting them without paying.^[14] Hackers allege that Avid Life Media received \$1.7 million a year from people paying to shut down user profiles created on the site. The company falsely asserted that paying them would "fully delete" the profiles, which the hack proved was untrue.”^[14] Wikipedia - https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

Weaponization of information

Weaponization of information can also be done by nation states, criminals or individuals for various motives. For example, in April 2013 the twitter account of the Associated Press was hacked. The account posted “Two explosions in the White House and Barack Obama is injured.” The stock market dropped 150 points.

Impact of Data Injury

Medical ID theft

Healthcare with impact on live itself– The victim may be misdiagnosed, mistreated, prescribed the wrong medication, delays in receiving appropriate care, and have virtually permanent errors in medical records. For example, victim may receive medication allergic to, or conflicts with existing medical regiment or not receive appropriate medication based on erroneous information in medical records. Perpetrators have received transplants via medical identity theft. A major risk is with emergency medical treatment where the victim may not be in a position to explain the existence of the fraud. For example: in emergency room in comatose condition and medical record has incorrect medical history - blood type, medical history (diabetes, heart conditions,), medications....

Out-of-pocket cost on average per victim. Unlike financial identify fraud, medical identity fraud does not have similar regulatory or legal consumer protections to limit liability of the victim. The victim has to manage the remediation of financial medical fraud losses unlike Fair Credit Billing Act that limits ID theft victims to \$50 loss.

Ponemon Institute, LLC estimated in 2015 2.3 million adults were affected by medical ID theft. Victims may not become aware of the theft until the bills begin to arrive.

The thief's health data can become folded into the victim's medical records. Often the victim cannot fully examine the medical records because of medical privacy laws protecting the perpetrator.

Wanda Aquino's identity was stolen identity was purchased for \$1,500. The perpetrator received a liver transplant under Wanda's identity. The perpetrator received only 6 months in federal prison.

<http://www.tmj4.com/news/i-team/medical-identity-theft>

For more details on medical identity theft refer to: MIFA report Nov. 2016 report - *Healthcare Industry Wisdom on Medical Identity Fraud*

Reputational impact

The victim may be impacted by the release of sensitive medical or health information publicly disclosed. The disclosed information may or may not be true.

Employment/livelihood - Victim may suffer negative employment issues with disclosure such as job loss, loss of advancement or loss of professional license when employment is based on condition related to health such as being drug free. For example, if perpetrator uses drugs and victim works for the U.S. government with security clearance.

US States Identity Theft Information and Identity Theft Registry

Driver license created with stolen PII has become such an issue that some states (i.e. Colorado, California) now have websites to assist in dealing with the aftermath of Including how to file a motion of factual innocence. Additionally, California has an identity theft registry for victims of identity theft.

Information Injury Framework

We propose a framework for protection of data similar to the NIST Cybersecurity framework requiring Identify & Protect the data, Detect when data or identity is compromised, Respond to & Recover from a compromise. The tools do not exist for a person or a consumer to be able to effectively perform the necessary steps to effectively implement the framework.

The first step is for all organizations that have information involving identities should be required to meet a minimum set of standards to protect the identities involved. Data aggregators, credit monitors, loyalty programs, are a few examples of whom should be required to comply.

Requirements should include the following:

- Right to be forgotten
- Right to free 24x7x365 access to all information involving your name & identity
- Ability to track all uses of your PII
- Ability to easily deny uses of PII
- Able to remove from "uses" at a later date
- Right to timely correction of information
- Default is to remove all information requested until formal determination

- Able to prevent private companies from tracking digital life/footprint
- Specific to companies that provide credit monitoring services
- Default status should be frozen credit
- Ability to unfreeze credit should be via an online/mobile application that supports quickly and easily turning on and off all freezes
- Companies collecting data without consent should not be able to profit from protection of identities or PII
- FTC “Red Flags” program requiring companies to detect identity theft includes civil monetary penalties. These should be expanded to include criminal penalties.

All organizations that store information on identities should be required to:

- Have field level encryption
- Segregation of duties
- Access to data on a Need to know basis only
- Admin accounts cannot access data
- Strong authentication (i.e. Multi-factor authentications) should be required for all access to data

Users of systems can access only a subset of data required to perform role

- Solution to detect exfiltration of large amount of data
- Solutions to prevent exfiltration of large amounts of data
- Report compromises/breaches of data within 72 hours to those affected
- Have incident response plans including steps to communicate with customers effectively and run table top exercises
- Create national identity theft registry for victims

Biometric Information Privacy Act

... “one state has already pre-emptively enacted legislation intent on protecting consumers’ privacy in light of new advances in biometric technology. Illinois’ Biometric Information Privacy Act (BIPA) prevents violations of citizens’ privacy rights where things like fingerprints, facial recognition, retinal scans, and other identifying body traits are concerned.”

<http://www.idtheftcenter.org/Privacy/biometric-facial-recognition-and-social-media-photo-tagging-heads-to-court.html>

Data protection is a shared responsibility and businesses and individuals should partner to protect their information.

For Businesses

Protect What is Collected

Businesses that collect, process and store information either of their employees, customers or vendors should be strictly liable for the protection and disposal of that information.

Data/Privacy breach should be included as a failure of design and operation of internal controls under Sarbanes Oxley Act, section 302. This will ensure that controls are adequate and tested regularly, and management will take a significant interest in the cybersecurity posture of the business.

Internal Documentation/Processes

Misinformation, limiting factors of poorly designed data fields and data models, often organizations are required to use oversimplified often-times incorrect fields and metadata that do not accurately describe complex situations. For example - insurance company issues refunds and then marks the client's account as cancelled due to nonpayment, when that was not the case, the payment was made, and then refunded, contrary to the client's wishes.

Impact of a Data Breach to the Business

Businesses should be aware of the disruption caused by a cybersecurity attack against the company's infrastructure. Most common and visible impact is a loss of customers business, cost of investigations and legal defense (IBM & Institute, 2017). However, inbound contact, outbound contact, and provision of free and discounted services resulting from a data breach can also add up.

Mandatory Cyber Insurance

Just as car drivers should obtain compulsory insurance for their vehicles and businesses are currently mandated to purchase workers compensation insurance, it should be compulsory for all companies that to buy insurance to mitigate the financial impact of Cyberattacks.

The top three reasons underwriters decline cybersecurity insurance are (Barbara Filkins, 2016):

- Inadequate cybersecurity testing procedures and audits 44.7%
 - Inadequate processes to stay current on new releases and patches 40.4%
 - Inadequate cyber incident response plan 38.3%
- Until better estimates and figures for per record loss in dollars is available a national amount of fine per loss of data record (a record means PII of an individual) should be assigned.

Once a business can quantify the amount of loss they will be liable for, they can implement and test controls around data input, storage, and destruction.

Summary

Information injury comes in many forms adversely impacting larger and larger numbers of people and business annual. Processes such as industry best practices, regulatory requirements, and laws are key to addressing the appropriate use of information, security of information, privacy and data. We propose development of a framework similar to the NIST CyberSecurity Framework for information injury prevention giving people, consumers and businesses, the ability to Identify all existences of their PII, Protect it, Detect compromises, effectively Respond to a compromise and Recover from a compromise.

A collaboration of the FTC and industry associations (i.e. IDESG - Identity Ecosystem Steering Group) to develop a framework that meets the needs of all stakeholders.

These comments are prepared by **Bev Corwin, Cindy Cullen and Niloufer Tamboly** members, International Committee of The Identity Ecosystem Steering Group (IDESG).