MIGNOLET
BUSINESS RESEARCH CONSULTANTS, INC.

In This Issue

Discovering text messages
Data Brokers' Categories

For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit: www.Mignolet.com

Contact us at:
investigators@Mignolet.com
or call us at: 954-523-8737

Quick Links

Our Website

Jean,

Who's Selling Credit Cards from Target?

They are being sold on an online fraud shop with the nickname 'Rescator', who allegedly runs another Russian and English crime forum. He has multiple online stores, and they all sell information from stolen credit cards.

In the past, KrebsOnSecurity has featured stories about banks buying back credit and debit card accounts stolen in the Target hack.

Be diligent!

Jean Mignolet

A reminder that prior issues of the newsletter are viewable from my website.

What Categories do the Data Brokers

Services

Join Our Mailing List!

E-discovery and evolving Text Messaging

E-discovery is a huge part of the legal system these days, and an important part of it is related to texting. It's becoming more important and offers a ton of legal implications in civil cases.

Divorce cases, contract law and personal injury cases are prime cases for texts to aid with the action at hand. Were you texting while driving? Did you end a string of contract infused texts with a positive expletive? Could be you have a contract at hand...see CX Digital Media, Inc. vs. Smoking Everywhere, Inc. (S.D. Fla. Mar. 23, 2011) where the word "Awesome" led to a $1.2 million judgment.

These messages need to be identified, collected and preserved; and don't forget about the photos, videos and other images. CDRs, Call Detail Records, include

have you in?

A data broker collects data on citizens, putting them into categories. Let's start with a list of a few of those categories, understanding that there are many more:

* Burdened by debt;
* Mid-Life strugglers;
* Struggling elders or singles;
* Young single parents;
* Resilient renters;
* Rural and barely making it;
* Financially challenged;
* Credit reliant;
* Living on loans;

and many other categories those citizens may live under.

The list is used to target products to a financially vulnerable populous.

An extensive report was released by a Senate committee which explains what a data broker, and companies that trade in consumer data, will not talk about. Their strategies for organizing and collecting data remain close to the vest. Likewise they will not reveal where they send it.

Some of the companies included in the report are trading in consumer data, such as Experian and TransUnion, and that's a bit unnerving. What are they collecting, how specific is it, how do they collect it, and how is it used? Substantial answers for the how they collect it and how it's used is still a mystery.

Previously companies would collect zip codes for

metadata which can be tracked by breaking down a call or text.

EDRM or Electronic Discovery Reference Model is a phrase for the preservation of electronically stored information or ESI. Forensically just about anything can be retrieved; most of us don't delete our text messages. You must comply with Court Orders, of course, but litigants are finding that even asking for this information may be obtained during those first meetings.

Everyone knows it's there. Mobile Chat Apps are third-party messaging services that don't use SMS delivery systems by pushing messages through data connection; there may be a log on the App but most likely it may not be stored.
"Over-the-top" is deployed in popular apps like iMessage, Blackberry Messenger, Skype, WhatsApp, Kik and others; and texts sent through an AT&T network, for example, might not appear in the text/SMS Call Detail Record. It varies with each service capturing transactions as data sessions within their operating systems. Some of the messages can occur over a Wi-Fi access point offering no associated CDR for evidence. Therefore, the best bet is to grab the info right off the mobile device.

When obtaining CDR, you have to look at the original and intermediary locations of the data so it starts with the device, the carrier and other repositories. Forensic examinations of cell phones have been used for over 20

marketers to send out catalogs and to target market consumers; but, now, data which includes financial is now being resold.

A company named Datalogix claims to have data on "almost every US household." Disturbing as this is, Acxiom, another data collecting company, claims to have data on over 700 million people worldwide. This includes what you purchase, the transaction information, how you pay, what type of car you buy, health conditions and your social media usage. Equifax claims that it even knows what type of shampoo you buy and possibly how many alcohol drinks you have had.

What the companies will not specify is where their sources for such consumer data are coming from. Acxiom, Experian, and Epsilon would not reveal the sources of their data because they have confidentiality clauses in their contracts.

Can you say "let's take a closer look"? Free government and public databases, together with licensed data purchases from retailers, banks, and other data brokers, are some of the sources we now know of. They are described lovingly as "third-party-sources."

Facebook once asked a data broker named Rapleaf to destroy the data it obtained by crawling the website. However, **Facebook and Google re-sell data fed to their services by customers to third parties like these data brokers.** The consumer remains anonymous in this instance. The next time you are a website, check out their privacy policy and you will see that over a quarter million of those sites state that they share data with other companies. You might want to think twice about using them.

years now focusing on call logs, contacts, SMS, calendars, browser history and the like, while third party OTT chat apps create activity logs written to SQLite databases that can be stored on removable media like a Secure Digital card.

Social Media and e-discovery professionals are dealing with online, third party providers but collecting data from the device itself seems to be the best option. Collect, process, review, analyze, and third-party server logs are integral parts of your e-discovery.

Don't forget that the option to now bring your own device to work makes it even more difficult to capture what you need for a case while holding true to the existing laws that cover e-discovery.

In closing, remember to hire professionals for forensic collection of e-discovery and think before you send out information.

Of course, there is always the "OPT OUT" option, correct? Hardly! Very few brokers even offer that option, and brokers frequently buy and sell their data from one another so they have a continuous stream in information coming in.

Where you opted out from one, you are NOT opted out from another.

Currently, there is no legislative movement regarding this issue, but the report does encourage policymakers to be aware of data brokers and what they are doing. They are reminding them that consumers have no legal protection against either data collection or a legal right to know what is being bought and sold.

So how do you cope? Expect it and know that judgments about your characteristics and predicted behaviors are out there!!!