WINTER 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss third-party keyboards on smartphones for emoji usage, keylogging and protecting your digital keystrokes. We also discuss the California Consumer Privacy Act of 2018 and its impact on our industry.

California's New Privacy Law: The New Standard?

On June 28, 2018, California Governor Jerry Brown signed the California Consumer Privacy Act of 2018 into law. The date is significant for two reasons. First, on June 21, 2018, bill AB-375 was resurrected after being declared "inactive" for almost a year. Within a week, the bill was modified, passed by both the California State Senate and the State Assembly, and signed into law by Governor Brown. The second reason, which we'll discuss below, provides an interesting insight into legislative motivation: flexibility in lawmaking. In this article, we'll review how the California Consumer Privacy Act of 2018, ("CCPA") came to be, what the CCPA does and doesn't do, and what the ramifications may be for both Californians and others.

The California Ballot Initiative

As we said above, the second significance of the June 28, 2018 date may be the key to explaining why the CCPA was passed into law with lightning speed. June 28, 2018 at 5pm was the deadline set by California real estate developer Alastair Mactaggart and the group he founded and funded, Californians for Consumer Privacy ("Cal Privacy"), for California's state government to either pass a bill which addressed consumer privacy, or see the matter go to a ballot initiative. The Cal Privacy organization gathered, more than double the required number of signatures in just five months, positive proof of the interest California residents had in protecting consumer privacy.

One of the main questions that arises is why was it so important to take the matter up as legislation, even at the last minute, rather than let the ballot initiative proceed? From the perspective of the legislators, it may have been a question of flexibility. Ballot initiatives passed by California voters are law, amendable only by subsequent ballot initiatives. Once approved by voters, legislators can do little to change the new law.

From Cal Privacy's perspective, despite the encouraging number of signatures collected, there was still a long way to go before the vote. This initiative would face a harsh fight for support in a state home to many of the companies which would be affected by the new law if passed by voters. If the key components of the initiative could be passed via legislation without the expense and bitterness of a campaign, the Cal Privacy organization could take that as a win.

The CCPA: The Toughest in the Nation

Irrespective of motivation or speed, the CCPA stands out as the current high bar for consumer data privacy protection in the United States. The California lawmakers and the Cal Privacy group crafted, in a short time, a bill that delivers the following protections to consumers:

1. The right to detailed information on what data is being collected by a business, without cost to the consumer, twice a year.
2. The right to opt-out of having personally identifying data sold.
3. The right to delete data posted about the consumer.
4. A provision for consumers to sue companies that do not adequately protect personally identifying data.
5. Protection from being denied service or up-charged because a consumer disallows data sale.
6. Notification of what types of data are being collected prior to and when collected, as well as, notification of any changes in collection practices.
7. Safeguards for minors, including opt-in versus opt-out permissions on data sales.
8. Disclosure of to whom data will be sold, the source of the data, and the reason for which it is being collected.

Businesses subject to the CCPA are those which do business in California, and:

1. Achieve annual gross revenue in excess of $25 million; or
2. Collect, buy, receive, sell, or share the personally identifying data of 50,000 or more California residents, households, or devices; or
3. Fifty percent or more of annual revenue is generated by subject data sales; or
4. Any business which is owned, operated, controlled, or "shares common branding" with a company that otherwise meets the above-listed prerequisites.

The text of the bill is found on the California legislative information page at the following link: *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375*.

The civil penalty imposed upon companies for breaches and violations is set at a maximum of $7,500 per incident, with the definition of exactly what comprises an individual incident left ambiguous. For consumers adversely impacted by a breach, the maximum statutory award is $750 per incident, although there is no cap on verifiable actual damages and injunctive relief is left to the judge's discretion. While the CCPA gives consumers some sweeping rights and the standing to sue, it should be noted, however, that should a consumer wish to sue for statutory damages, notice provisions and a cure period may prevent a suit from reaching the courtroom.

More Questions than Answers?

Interestingly, the provision to protect the personal information of minors is more proactive than that for adults, and some critics question why it wasn't made the law's universal standard for all personally identifying data regardless of the subject's age. For minors under 16, the data cannot be sold unless express permission to do so is granted via opt-in, and for those under 13, the opt-in must be elected by a parent or guardian. In what may seem like a compromise to the issue of adults having to opt-out, subject businesses are required to post "Do Not Sell My Personal

Information" links on business homepages, and to establish toll-free phone numbers for consumers to call to opt-out. Businesses must also respond to requests under the law within forty-five days.

Another apparent dichotomy of the law is that while consumers may not be penalized for opting out via either reduced/denied service or pricing penalties, businesses may offer financial incentives to induce consumers to allow the sale of personal information, provided those incentives do not conflict with the prohibition against penalizing consumers. This begs the question of how exactly a financial incentive to sell data will look in comparison to pricing for services without data sales? For example, would a statement credit for data sales violate the pricing provision in that it effectively changes the price of the service by offering a rebate in exchange for selling data?

Finally, the CCPA includes biometric information as part of the protected information, including retinal scans, iris scans, fingerprints, voice recordings, and DNA profiles, which raises the question of whether popular DNA analysis companies will find sharing DNA information with insurance companies troublesome, whereby possibilities existed for personal data usage. Under the terms of the law's text, a prospective DNA analysis client could request that their genetic information not be sold. If true, does that extend to government law enforcement agencies as well? In April 2018, California law enforcement officials announced that they had used information from an online genetic profiling service to find a genetic match for a relative of the Golden State Killer, which led to a suspect's arrest decades after the crimes.

Spreading the Word

The effective date of the CCPA isn't until January 1, 2020, although an amendment has already been passed allowing California's Attorney General ("AG") until July 1, 2020 to promulgate regulations under the law and removes the AG's ability to intercede in private lawsuits. Additionally, the amendment precludes the AG from pursuing violations of the law for six months after the effective date. The US Chamber of Commerce ("USCC"), the Interactive Advertising Bureau, and the Internet Association are all lobbying at the federal level for legislation that will override the CCPA. On January 10, 2019, the USCC posted their platform for a national privacy law which protects businesses from being sued by individuals and advocates for actual damages only penalties, (*https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf*).
Until such time as there is a nationwide data privacy law, the word is spreading about the CCPA, and other states are considering their own bills. Nine other states have passed new data privacy laws or amended existing ones in 2018. Fast or slow, a new standard of privacy for personally identifying information is coming.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ABA TECHSHOW 2019
Chicago, IL: February 27, 2019 - March 2, 2019

MASTERS CONFERENCE
Dallas, TX: February 28, 2019

THE SEDONA CONFERENCE WORKING GROUP 11 ANNUAL MEETING 2019
Houston, TX: February 28, 2019 - March 1, 2018

RSA CONFERENCE 2019
San Francisco, CA: March 4-8, 2019

THE ASU-ARKFELD 8TH ANNUAL EDISCOVERY
Phoenix, AZ: March 6-8, 2019

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: