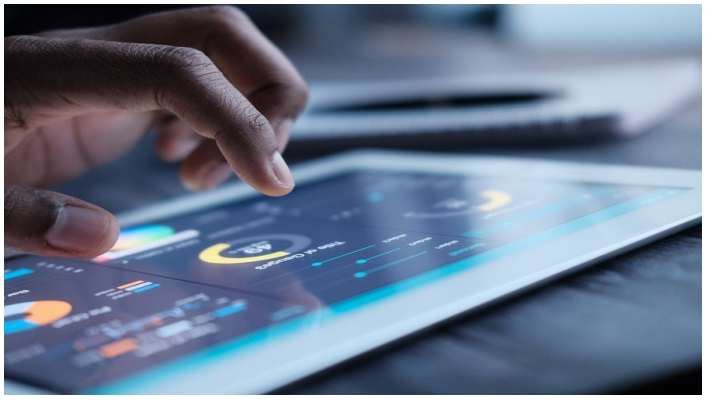
Identity verification and privacy in the time of pandemic

07 AUGUST 2020

M. Ridgway Barker
PARTNER | US



CATEGORY:
ARTICLE

CLIENT TYPES:
TECHNOLOGY

FINANCIAL SERVICES

DIVORCE

INNOVATIVE FINANCING

DATA PROTECTION

CRYPTOCURRENCY

FINANCE

BLOCKCHAIN

DATA PRIVACY

COVID-19

CPPA

PRIVACY

DATA

IDENTITY

M. Ridgway Barker co-authored this article with Joseph Bambara CIPP/US.

An INTERPOL (interpol.int) assessment of the impact of COVID-19 has shown a dramatic increase in cybercrime not only against individuals and small businesses but to all major corporations, governments, and critical infrastructure. The Financial Crimes Enforcement Network (FinCEN) has also issued an advisory alerting financial institution to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are taking advantage of increased security vulnerabilities to breach security and steal data to generate profits and cause disruption. According to INTERPOL, just one private sector partner in the period of four months between January to April of 2020 experienced some 907,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs – all related to COVID-19. We need to counteract this new development with increased efforts to protect the privacy and identity of personal data. We not only need privacy legislation, but we need to upgrade our old and obsolete identity verification technology to address this new pandemic enabled cybercrime wave.

Over the past few years, we have seen a progressive movement for protecting the privacy of personal data around the globe. The EU General Data Protection Regulation (GDPR) took effect in May 2018. The California Consumer Privacy Act (CCPA), which became a law in June 2018, took full effect on January 1, 2020. Before the pandemic, data privacy legislation was a focus for many state governments throughout 2019, including New York, Massachusetts, Texas, and Washington. Maine and Nevada have passed their own privacy laws. On both the House and Senate side, the US Congress has released discussion drafts of broad federal privacy legislation.

Let's examine the CCPA as it is a potential model for other state and federal legislation. The Act intends to provide California residents with the right to know what personal data is being collected about them and the ability to access, delete and control whether their personal data is sold or disclosed and to whom. The CCPA defines personal information ("PI") as any data that can be in any way used to identify an individual or household. This definition is inclusive of things like name, alias, postal address, Internet Protocol address, email address, social security number, driver's license number, passport number, or other similar identifiers.

Enterprises were required to be fully compliant with the CCPA by July 1, 2020, when enforcement officially went into effect. The CCPA applies to enterprises that collect consumers' personal data does business in California and has annual revenues of over $25 million or collects the PI of greater than or equal to 50,000 consumers or earns a simple majority of its annual revenue from selling PI.

If your enterprise falls into one of these categories, you are required to "implement and maintain reasonable security procedures and practices" in protecting consumer data. This translates to functionality your public-facing platform must also implement processes to obtain consent for

minors under 13 years and the affirmative consent of minors between 13 and 16 years to data sharing for purposes. You will need to provide a link for "Do Not Sell My Personal Information" to opt-out of PI sales. In addition, there are a number of other requirements addressing PI data access requests, privacy policies, and opt-in / opt-out rules.

There are several sanctions and remedies that apply. Enterprises that have been data breached may incur statutory damages or any relief a court deems proper, subject to an option of the California AG to prosecute. Fines of up to $7,500 for each intentional violation and $2,500 for each unintentional violation.

Unfortunately, the July CCPA enforcement deadline comes as the COVID-19 pandemic continues changing priorities as information technology professionals are forced to work remotely and business has shifted online. For businesses to survive the pandemic, the digital customer experience is now the priority. On top of this, information technology professionals are under tremendous pressure to ensure applications and infrastructure remain secure across the new remote workforce with tightened budgets and limited resources.

Data privacy professionals have seen increased CCPA rights requests amid the pandemic. As operations have shifted online, it is a challenge to verify that the person making the rights requests is, in fact, the true owner and not a cybercriminal. This has put enterprises at risk to be victimized by fraud while complying with CCPA. As California consumers are trusting enterprises with the disclosure, deletion, and collection of their personal data, these enterprises must maintain this trust by keeping personal data out of the wrong hands. Under the CCPA, consumers have the right to pursue lawsuits if their data is exposed, with statutory damages ranging from $100 to $750 per consumer per incident, or the cost of actual damages caused by a data breach, whichever is more.

Owing to the numerous data breaches and phishing attacks, PI is relatively easy to find. Once cybercriminals purchase this information using browsers like TOR ("the onion router") to access the dark web, they can log in to your bank or credit card accounts, change passwords, lock the real user out, make fraudulent purchases and transfer funds. Using a password-protected account to submit a CCPA rights request makes it impossible to know if the requester is legitimate or a cybercriminal accessing the account with exposed, purchased data from the dark web. If enterprises do not have proper identity verification tools in place confirming the user is the person they claim to be, enterprises can share personal data with a cybercriminal without even realizing it. This ultimately subjects them to compliance fees, lawsuits, and loss of trust from their customers.

The Need for new Digital Identity Verification

Besides legislation, we also need new digital identity verification technology. Also known as "identity and access management", or IAM, identity management comprises all the processes and technologies within an organization that is used to verify, identify and authenticate/authorize someone to access services. So, with respect to the CCPA to maintain this trust while securely complying, organizations must be able to verify a user's digital identity with each rights request. If a user can set up an account with simply a name, phone number, and email address, anyone with this information can submit a CCPA rights request, not just the account owner. Biometric authentication is perhaps a reliable way to ensure data is shared securely. Also requiring a user to submit a photo of a government-issued ID and a real-time photo when opening an online account along with a corroborating photo each time they log in and make a request, organizations can confirm the person making the request is the true account owner. This authentication method is also more secure than passwords and SMS-based two-factor authentication, but it is tedious and can also be compromised.

Today digital identity is typically stored on a centralized server. It is a honeypot for hackers. As discussed earlier, since 2017 alone, more than 600 million personal details such as addresses or credit card numbers – have been hacked, leaked, or breached from organizations. Most of the current identity management systems are weak and outdated. Identities need to be portable and verifiable everywhere, any time, and digitization can enable that. But being digital is not enough. Identities also need to be private and secure to protect individuals and their families. COVID task force leader, Dr. Anthony Fauci has said he and his family have required continued security in the face of harassment and death threats from people angry over his guidance on the coronavirus pandemic. Others like Federal Judge Esther Salas have issued a call for increased privacy protections. A criminal found the Judges Salas address and other personal information online and came to her home, killed her son, and severely injured her husband.

Fortunately, new technology is becoming available to protect our PI and identity. Blockchain identity software is used for both identity management and identity verification. These platforms are built on a blockchain or distributed ledger system that provides improved traceability and documentation over traditional identity management solutions that rely on centralized systems. Because these tools are built upon blockchain-based ledgers, every activity and change made by an individual is documented on the blockchain. Companies use these tools to first ensure that identities are accounted for and protected. Furthermore, businesses use these tools to build a historical record of activity and risk to be used when identifying suspicious behavior or transactions. Many blockchain identity tools rely on zero-knowledge verification, meaning identities are verified without presenting any sensitive information about the individual. Zero-knowledge verification allows users to build out passwordless authentication systems and zero-knowledge proofs for identities. A Zero-Knowledge Proof is a method of authentication that, through the use of cryptography, allows one entity to prove to another entity that they know a certain piece of information or meet a certain requirement without having to disclose any of the actual information that supports that proof. The entity that verifies the proof has thus "zero knowledge" about the information supporting the proof but is "convinced" of its validity. This is especially useful when and where the prover entity does not trust the verifying entity but still has to prove to them that he knows a piece of specific information. See, https://www.g2.com/categories/blockchain-identity for a list of the best blockchain-based identity software.

As other states have begun to follow in California's footsteps in creating similar consumer privacy laws, enterprises would also be wise to adopt "best of breed" digital identity verification solutions that offer data security, transparency, and retention policies that comply with CCPA and any new legislation. With expanded rights come expanded enterprise responsibilities, and enterprises must retain trust to protect both their business and their consumers. The combination of well-designed legislation and technology can solve most any new challenge to our privacy and prosperity.

Our Withers attorneys can assist and educate clients from a legal and technical standpoint to incorporate these emerging technology trends safely and efficiently to help your businesses stay ahead of the competition. Please contact your regular Withers attorney or the author of this piece with any questions.

Authors

M. Ridgway Barker

PARTNER | GREENWICH

Corporate

+1 203 302 4084

mr.barker@withersworldwide.com