Privacy, Data and CyberSecurity: Updates You Need to Know for 2021

By Culhane Meadows's Privacy, Data & Cybersecurity Practice Group
January 27, 2021

In honor of international Data Privacy Day on January 28, 2021, members of Culhane Meadows's Privacy, Data & Cybersecurity Practice Group are highlighting a few recent legal developments, surprises, and resources you will want to have on your radar screen in 2021. More information about Culhane Meadows's Privacy and Cybersecurity services is available at: https://www.culhanemeadows.com/privacy-data-and-cybersecurity/.

Let us know if you have questions or would like more information. We look forward to assisting you.

The California Privacy Rights Act (Sally L. Byrne, CIPP/E/U.S./M, Partner)

The California Privacy Rights Act ("CPRA") was created by California ballot initiative on November 3, 2020. It substantially revises and replaces the California Consumer Protection Act ("CCPA") that went into effect January 1, 2020. Most of the substantive requirements of the CPRA will become effective on January 1, 2023, but under a look-back clause some of the provisions will apply to data collected on or after January 1, 2022. Key features of the CPRA include:

- A new category of "sensitive personal information" and limits on what can be done with this information.
- A right to correct inaccuracies in consumer personal information.
- Expansion of penalties for the collection and use personal information regarding children under the age of 16 and strengthened opt-in rights.
- Expansion of the opt out right for the use of personal information to apply to selling *and sharing* of personal information (as opposed to only selling under the CCPA).
- Expansion of data breach provisions to apply to email and password combinations.
- Extension of the employee and business to business exemptions that were provided under the CCPA.
- New data retention requirements.
- Mandatory audit and assessment requirements for certain high-risk activities.

A significant change under the CPRA is the creation of California Privacy Protection Agency which will have the authority to implement and enforce the law. This is the first agency in the United States to be directed solely to privacy rights.

New DOD Contractor CMMC Interim Rule & NIST 800-171 (Linda V. Priebe CIPP/E, Partner & Privacy, Data & CyberSecurity Practice Group Chair)

The new U.S. Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) Interim Rule, 85 FR 61,505, which went into effect very quickly on November 30, 2020 included an unexpected surprise for 20,000 DOD Prime and Sub-Contractors. The CMMC's enhanced compliance requirements had already gotten a lot of attention from DOD contractors so the interim rule was not a surprise and will be gradually phased in until 10/1/2025. The surprise in the CMMC Interim Rule is the DOD's new enforcement mechanism for the NIST SP 800-171 DOD Assessment. The Interim Rule requires contractors to perform a self-assessment

of each of the NIST 800-171 110 weighted cybersecurity controls and report their score in the DOD Supplier Performance Risk System prior to being awarded a DOD contract beginning December 1, 2020. Compliance with NIST SP 800-171 being required by DOD contracts is not new, but previously compliance was satisfied merely by contractors' self-attestation and the DOD rarely conducting reviews. This is a whole new world of cybersecurity compliance accountability for DOD contractors and sub-contractors. Other U.S. Government agencies including the General Services Administration are also considering adopting the DOD's new approach to cybersecurity compliance.

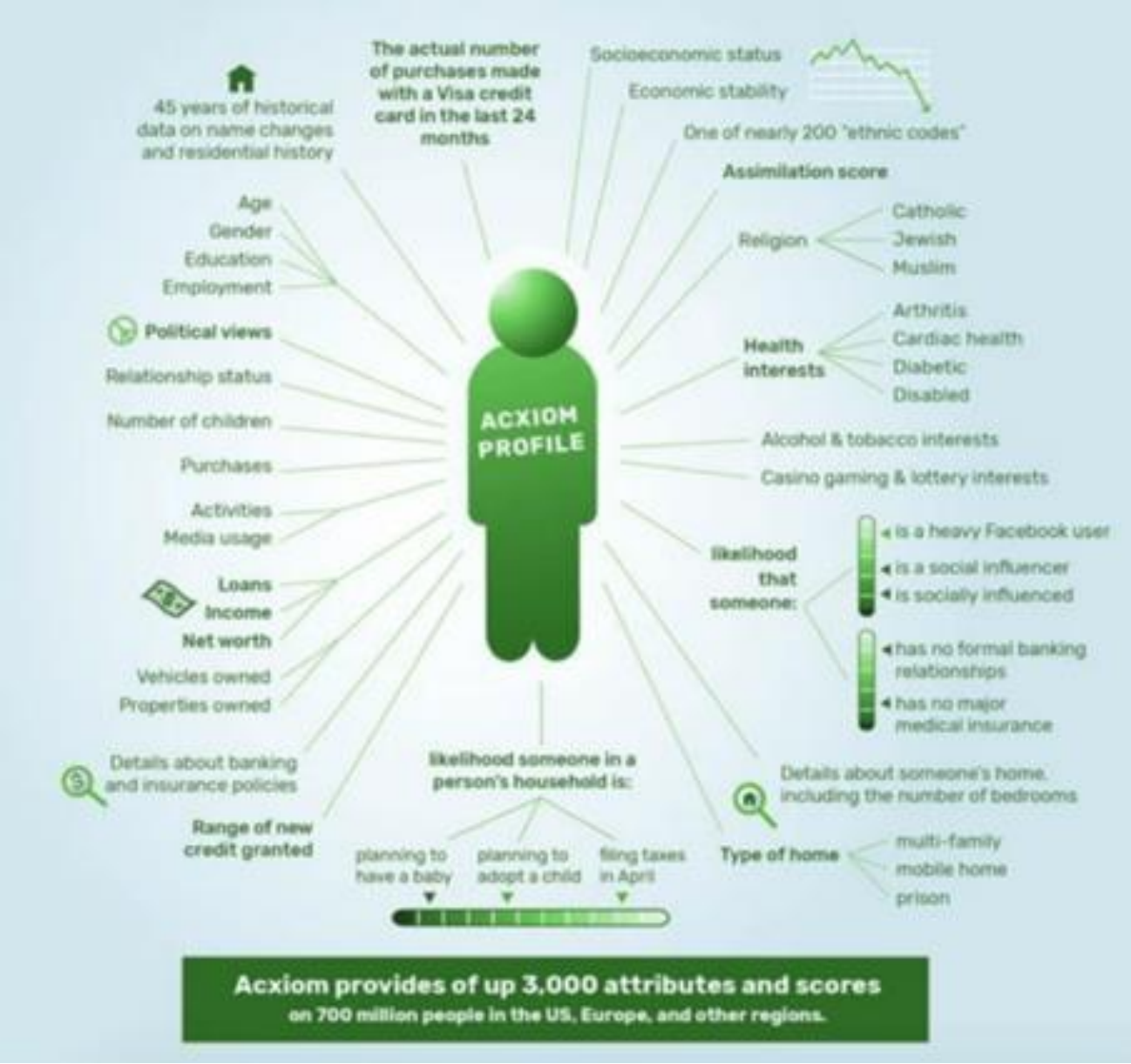
US Court PACER System Suspected Russian Hack (David Jacoby, Partner and International Practice Group Chair)

The believed-to-be Russian hacking of various federal agencies through Solar Winds has raised concerns about possible exposure of highly sensitive documents filed on the federal court system's Case Management/Electronic Case Files system, which supports the publicly searchable PACER database. One report has suggested that a second form of malware was inserted that also affects PACER. More disturbing still, it wouldn't be the first intrusion into PACER. One which allowed unauthorized free users to piggyback on legitimate users' requests was corrected in 2017. Another hack by Ivy League students and the Internet Archive occurred in 2009. While most federal court cases don't involve national security data, many do turn on documents that are highly sensitive for commercial or technical reasons. The Administrative Office of the U.S. Courts issued a statement on January 6, 2021 that an "apparent compromise" of CM/ECF confidentiality was under investigation. A number of the over 200 federal courts PACER covers quickly issued orders setting up special procedures for filing highly sensitive documents. Practitioners will need to check court-by-court where they have pending matters, because the procedures are not uniform. For example, in the District and Bankruptcy Courts in the SDNY and in the District of Columbia District Court, the orders establish a procedure for a party to move to have a filing treated as involving highly sensitive documents which then would be filed with the court in hard copy and on a thumb storage medium placed in a conspicuously labelled sealed envelope.

Surprisingly Legal Practices Under Current U.S. Privacy Laws (Kim Verska, CIPP/U.S., Partner and Privacy, Data & CyberSecurity Practice Group Chair)

Among the personal data that companies have recently been found to routinely sell to third parties while staying within the letter of current U.S. law include: location data from your telco provider (recently mostly curtailed under FCC pressure); sensitive data about your health from app providers not covered by HIPAA; and data from your profile and use of social media, as famously revealed in the Cambridge Analytica scandal (Facebook and your profile). Are you surprised by any of the above? Here at the start of 2021, U.S. privacy law still remains a patchwork with major holes outside of specific regulated industries and activities, even as other countries emulate the EU in passing data protection laws like the GDPR that apply generally to all processing of personally identifiable data. The foundational hole in U.S. privacy law is (and you may be surprised by this too) that there is currently no federal law requiring that a company publish a notice of its privacy practices, much less grant you consent rights over the additional and very profitable uses being made with data about you. Your gut is right: everyone, everywhere is directing targeted marketing to you all the time, and it is in large part thanks to data brokers such as Acxiom, Oracle and the three credit reporting giants. Acxiom alone maintains up to 3000 data points on 700 million people worldwide, and they sell these individual profiles to advertisers and others (see the image below to see the types of data they collect and sell). Some states, most notably California, are acting to remedy this, but as the Biden

Administration and a Democratic Congress take office this month, it's worth asking how willing they will be to impose nationwide legal requirements on these kinds of uses of personal data, seen as the very engine of our "information economy." Only time will tell, and meanwhile, in honor of Privacy Day, here's a link where you can [opt out of Acxiom's sales of some of your data](#).



More Data Privacy/Protection Resources

Report on Data Privacy Regulations Applicable to Blockchain, INATBA, Dec 2020
(Contributor Caroline Morgan, Partner, Culhane Meadows) https://inatba.org/wp-content/uploads/2021/01/2020-12-Privacy-WG-Report-on-Data-Protection-005.pdf

National CyberSecurity Alliance https://staysafeonline.org/data-privacy-day/

The foregoing content is for informational purposes only and should not be relied upon as legal advice. Federal, state, and local laws can change rapidly and, therefore, this content may become obsolete or outdated. Please consult with an attorney of your choice to ensure you obtain the most current and accurate counsel about your particular situation.

About Culhane Meadows – *Big Law for the New Economy*®
The largest woman-owned national full-service business law firm in the U.S., Culhane Meadows fields over 70 partners in ten major markets across the country. Uniquely structured, the firm's Disruptive Law® business model gives attorneys greater work-life flexibility while delivering outstanding, partner-level legal services to major corporations and emerging companies across industry sectors more efficiently and cost-effectively than conventional law firms. Clients enjoy exceptional and highly-efficient legal services provided exclusively by partner-level attorneys with significant experience and training from large law firms or in-house legal departments of respected corporations. U.S. News & World Report has named Culhane Meadows among the country's "Best Law Firms" in its 2014 through 2020 rankings and many of the firm's partners are regularly recognized in Chambers, Super Lawyers, Best Lawyers and Martindale-Hubbell Peer Reviews.