



STAR STRUCK

NAVIGATING “REASONABLE SECURITY” UNDER CALIFORNIA’S CONSUMER PRIVACY ACT | [JUSTINE M. PHILLIPS, ESQ.](#)

California is the birthplace of stars, the Internet, and consumer privacy. In 1974, California empowered its residents with an inalienable constitutional right of privacy. Over time, that right has expanded to “shine the light” on mandatory online privacy policies and require consumer notices of data breaches (2003), and public shaming of companies for breaches impacting 500+ citizens (2012).

In 2018, California passed the California Consumer Privacy Act (“CCPA”), giving individuals the right to be forgotten and steep fines/penalties for failing to implement reasonable security. Businesses seeking to comply must implement “reasonable security procedures” and practices by January 1, 2020. But navigating a nebulous concept like “reasonable security” can feel like we are ships lost at sea. To find our way home, data must first be charted like luminous lights in the night sky—and we have much to learn from ancient astronomers.

THE LAW

The CCPA gives Californians the right to bring a civil action against a business for failing to “implement and maintain *reasonable security* procedures and practices appropriate to the nature of the information.” Statutory damages range from \$100-\$750 per consumer, per incident. Civil penalties by the

Attorney General may also be assessed at \$2,500 to \$7,500 per violation. The ethical and legal obligation to implement, “reasonable security procedures and practices” to protect personal information from unauthorized access is nothing new—but the damages and penalties give it some teeth.

REASONABLE SECURITY

The CCPA requires the California Attorney General to publish guidelines on just what “reasonable security procedures and practices” are. Although Attorney General Becerra has yet to issue such regulations, the 2016 Data Breach Report (“Breach Report”) released by former Attorney General Kamala Harris is our North Star. The Breach Report is clear: Failure to implement all 20 controls from the Center for Internet Security’s Critical Security Controls (formerly the “SANS Top 20”) that apply to an organization’s environment “constitutes a lack of reasonable security.” The Breach Report goes on to recommend multi-factor authentication, data minimization, and encryption as “reasonable security measures.” Yet, one cannot secure data until it is first identified, classified, and charted.

STARGAZING

If your ultimate destination is to safeguard your data and systems, then IG is your travel guide. Like ancient astronomers who began charting the stars thousands of years

ago, data mapping uses practical methods of observations to understand and chart the flow of data. Like stars, data is seemingly infinite, constantly expanding, and fills us with a greater sense of mystery and perspective.


Early astronomers did not use complex telescopes or software to map out the stars; rather, they looked up at the stars instead of down at their feet. Accordingly, businesses should observe the way employees and third-party service providers access and utilize data, identify where personal information is stored, and begin to map out their constellations of data.

MAPPING

To draw up your organization's data map, start with identifying the brightest stars like your customer database or invaluable intellectual property. After identification and classification, move on to specifying all the places that data is located. Information assets and data are often widely distributed and may reside on your servers, in the cloud, with vendors, on mobile devices owned by employees, and beyond. Data maps do not have to be fancy; instead, make them functional. Create the data map in a Word chart, Excel file, or Adobe Illustrator. Use a program that you can modify so the map evolves with additional information you learn about your data. It is only after we identify, locate, and classify the data that we can reasonably secure it.

CONCLUSIONS

Just as ancient astronomy evolved, our understanding of "reasonable security" will as well. The Attorney General is expected to promulgate regulations in the California Code of Regulations before CCPA may be enforced by the Attorney General in July 2020. The Attorney General's Office has indicated that it will rely on public comments in setting out those regulations and is conducting a CCPA rulemaking road show in January and February at various locations throughout California. Soliciting feedback from stakeholders in advance of drafting the regulations will hopefully lead to a standard of "reasonable security" that businesses can utilize on their journey towards compliance.

Until we have more guidance from the Attorney General, the Breach Report and data mapping will set the course. 



JUSTINE M. PHILLIPS, ESQ. IS A PARTNER IN SHEPPARD MULLIN'S SAN DIEGO OFFICE IN BOTH CYBERSECURITY AND LABOR & EMPLOYMENT PRACTICE GROUPS. JUSTINE TAKES A PRACTICAL AND MINDFUL APPROACH TO ASSIST HER CLIENTS IN EVERY ASPECT OF CYBERSECURITY FROM DATA IDENTIFICATION THROUGH DESTRUCTION, COMPLEX LITIGATION, AND PRIVACY/SECURITY BY DESIGN. SHE CAN BE REACHED AT [JPHILLIPS@SHEPPARDMULLIN.COM](mailto:jphillips@sheppardmullin.com).



GETTING SCHOOLED

U OF SAN DIEGO HOSTS CYBER LAW, RISK AND POLICY SYMPOSIUM

The University of San Diego's Center for Cyber Security Engineering and Technology (CCSET) hosted a two-day symposium last November on Cyber Law, Risk and Policy. This event brought together cybersec industry thought leaders to discuss how the law impacts corporate cyber risk and polices.

One specific topic was the on-going dialog generated by the California Consumer Privacy Act (CCPA). California is once again leading the nation in privacy rights, as the CCPA is, to date, the most sweeping state legislation governing cyber liability.

The CCPA requires the CA Attorney General to "solicit broad public participation" for input to be used to draft regulations to clarify portions of the law, prior to its implementation in 2020. The Symposium provided attendees with the opportunity to hear cybersec experts from law firms, insurance companies, security companies and law enforcement discuss their views on "reasonableness" and reflect on how the law should be and will be implemented.

The Cyber Law, Risk and Policy Symposium featured all-star speakers and panelists including representatives from: Microsoft, IBM, Capital One, AAA, the PCI Council, CompTIA, Cylance, SPLUNK, vArmour, FBI, US Secret Service, the US Department of Justice and the San Diego District Attorney's Office as well as professional service organizations, law firms and insurance companies. This stellar collection of presenters and panelists provided the 100+ attendees with the opportunity to learn real-world insights into cyber centric topics such as: *Live Data Breach & Ransomware Attack and Incident Response*; *Cyber Insurance: From Risk Transfer to Cyber Threat Response*; *Emerging Tech in the Law: Artificial Intelligence, Internet of Things and Blockchain*; and *Cyber Security and U.S. Elections and Cybersecurity Strategy: Raising the Risk Conversation*.

Organized by USD's CCSET (<https://sandiego.edu/engineering/cyber-security-center>) and spearheaded by a robust advisory committee of top cyber professionals, the *Cyber Law, Risk and Policy Symposium* represents San Diego's national leadership in the effort to get out in front of the evolving legal landscape of privacy regulations and their intersection with industry compliance regulations. Planning for next year's Symposium is already underway. To suggest topics or volunteer contact Justine Phillips via email at: JPhillips@SheppardMullin.com or jodiw@sandiego.edu.

—**Baird W. Brueseke** 