September 12, 2015

Governor Edmund G. Brown, Jr.
c/o June Clark

Re: SB 178 – SUPPORT CalECPA.

Dear Governor Brown:

The undersigned are legal scholars from throughout the United States who teach and write extensively about criminal procedure, information privacy law, internet law and related fields. We write in support of SB 178, which clarifies that California law requires that government entities obtain a warrant to access the electronic communications data we store on our cell phones and with our service providers, including read and unread emails, to-from data, and location information. By establishing a warrant requirement, this law will both protect the rights of Californians and provide needed clarity in this fast-evolving area of law.

Under SB 178, government entities must obtain a warrant, subject to limited exceptions, before they may compel the disclosure of electronic communication information from service providers or obtain such information directly from electronic devices. That requirement ensures that a neutral magistrate first finds probable cause before government agents conduct intrusive investigations into our private lives. Without a warrant requirement, Californians must generally rely on law enforcement discretion for the privacy and security of their electronic data. Judicial oversight helps ensure that law enforcement agents do not acquire, store, and potentially share more revealing electronic information than they need to investigate crimes and secure public safety. Only the protections of the warrant requirement can assure Californians that their use of essential modern technologies is free from unjustified government surveillance.

SB 178 codifies existing California constitutional principles. The California Supreme Court established decades ago in *People v. Blair* (1979) that law enforcement agents' collection of information sufficient to furnish a person's "virtual current biography," such as a record of telephone numbers dialed, intrudes on reasonable expectations of privacy. In *Blair*, the Court granted a motion to suppress a list of telephone numbers and explained the need, under California law, for "a judicial determination that law enforcement officials were entitled thereto." SB 178's warrant requirement applies *Blair* to the electronic equivalent of dialed telephone numbers, as well as information about the sender, recipients, contents, format, location, and time of communications, all of which easily furnish a virtual current biography. In addition, government access to electronic communications, location data and metadata implicate rights of free expression and free association, which the California constitution clearly protects. *White v. Davis* (1975).

Federal courts have required a warrant for some of the information SB 178 covers. In *United States v. Warshak* (6th Cir. 2010), the Sixth Circuit held that law enforcement agents must obtain a warrant based on probable cause when they compel a service provider to disclose the contents of emails it stores. The *Warsha*k court recognized that "email requires strong protection under the Fourth Amendment; otherwise the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve." By requiring a warrant for access to email content, SB 178 codifies not only *Warshak* but the practices of Facebook, Google, Microsoft, and other major providers.

The Supreme Court itself has held that law enforcement agents must either obtain a warrant to search a cell phone or establish exigent circumstances, just as SB 178 requires. Last year, in *United States v. Riley* (2014), the Court rejected the government's request to extend the search-incident-to-arrest exception to the warrant requirement to cell phone searches. The Court refused to apply to cell phone searches the

precedents established for the searches of purses and wallets because "that would be like saying a ride on horseback is materially indistinguishable from a flight to the moon." Recognizing that cell phones' storage capacity and multi-functionality mean they contain "the privacies of life," the *Riley* Court required law enforcement agents to "get a warrant" for cell phone searches. SB 178 codifies *Riley*.

SB 178's protection for location data also finds support in recent Supreme Court decisions. In *United States v. Jones* (2012), five concurring justices found that law enforcement agents intruded on reasonable expectations of privacy when they used a GPS tracking device to obtain several weeks of location data. The *Jones* justices recognized a privacy interest in location data even though it revealed the suspect's location out of doors and not inside a home. The *Jones* investigation involved acquisition of real-time data, but the *Riley* Court later recognized privacy interests in stored location data; "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[1]

Despite strong support for SB 178 in existing law, its passage will bring needed clarity for all those affected, including law enforcement. For example, legal uncertainty persists about the treatment of location data obtained from cell phone providers, despite the *Jones* decision. Congress has not updated the federal electronic surveillance laws that are nearing their 30th birthday. Those laws have been justifiably criticized for being more complex and convoluted than the tax laws and for being particularly a mess regarding location data. At the same time, government lawyers argue that under Fourth Amendment precedents from the 1970s, people forfeit privacy in information, such as location data, stored with third parties.[2] While the Supreme Court has not extended those precedents to modern communications technologies and its recent decisions suggest it may not,[3] the Court has not yet joined the California Supreme Court in rejecting the third party rule's application to electronic communications and metadata.[4]

Because of the persisting legal uncertainty, Californians have good reason to worry that the information SB 178 covers is inadequately protected. High technology companies cannot assure their customers that

---

[1] The Fourth Circuit recently found the warrantless acquisition of an extended period of stored location data from a cell phone provider to be an unreasonable search because it impacts a person's "interests in both the privacy of her movements and the privacy of her home." *United States v. Graham* (2015). The court viewed users' constitutional privacy interests in their historical location data as no different from such interests in real-time and prospective location data. "A person's expectation of privacy in information about where she has been is no less reasonable, or less deserving of respect, that that regarding where she is or where she is going."

[2] Two cases in the Northern District of California, like *Graham*, recently rejected application of the "third party rule" and required a warrant for law enforcement access to historic location data. *In re: Application for Telephone Information Needed for a Criminal Investigation* (2015) and *United States v. Cooper* (2015).

[3] In her concurrence in *Jones,* Justice Sotomayor explicitly disapproved of using the third party rule in cases involving new communications technologies.

[4] The court in *In re: Application* found reasonable expectations of privacy in location data based in part on the California constitution. The court explained, "there is little doubt that the California Supreme Court's holding [in *Blair*] applies with full force to the government's application here, which seeks historical [location data] generated by a target cell phone's every call, text, or data connection, in addition to any telephone numbers dialed or texted." As did *Graham*, the court distinguished two federal appellate decisions that required no warrant when agents acquired a much more limited set of location records.

they comply with law enforcement requests for user information under a set of rules that is both sensible and privacy-protective. The impressive coalition of companies and industry groups that support SB 178 suggests that SB 178's provisions are just that.

SB 178 incorporates into California statutory law legally sound provisions that are essential to ensuring that Californians may take advantage of innovations in communications technologies without sacrificing their constitutionally protected rights to privacy, free expression and free association.

Signed,[5]

California Scholars:

Susan Freiwald
Professor of Law
University of San Francisco
School of Law

Anupam Chander
Director, California International Law Center
MLK Jr. Hall Scholar and Professor of Law
UC Davis School of Law

Erwin Chemerinsky
Dean of the School of Law
and Distinguished Professor of Law
Raymond Pryke Professor of First Amendment Law
UC Irvine School of Law

Catherine Crump
Assistant Clinical Professor of Law
Associate Director, Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law

Jennifer Stisa Granick
Director of Civil Liberties
Stanford Center for Internet and Society
Stanford Law School

Kaaryn Gustafson
Professor of Law and Co-Director
Center of Law, Equality and Race (CLEAR)
UC Irvine School of Law

[5] All institutions are listed for identification purposes only and the signatories do not speak for or on behalf of their respective institutions.

Mark A. Lemley
William H. Neukom Professor
Stanford Law School
Director, Stanford Program in Law, Science and Technology
Senior Fellow, Stanford Institute for Economic Policy Research

Richard Leo
Hamill Family Chair
Professor of Law and Social Psychology
University of San Francisco
School of Law

Jack I. Lerner
Assistant Clinical Professor of Law
Director, UCI Intellectual Property, Arts, and Technology Clinic
UC Irvine School of Law

Stephen M. Maurer
Adjunct Professor of Public Policy
Director, Information Technology and Homeland Security Project
Goldman School of Public Policy
UC Berkeley

Sharon A. Meadows
Director, Criminal and Juvenile Justice Law Clinic
Professor of Law
University of San Francisco
School of Law

L. Song Richardson
Professor of Law
UC Irvine School of Law

Pamela Samuelson
Richard M. Sherman
Distinguished Professor of Law
UC Berkeley School of Law

Kurt M. Saunders
Professor of Business Law
California State University, Northridge

Steven F. Schatz
Philip & Muriel Barnett Professor of Law
University of San Francisco
School of Law

Jennifer M. Urban
Assistant Clinical Professor of Law
Director, Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law

Out-of-state Scholars:

Annemarie Bridy
Professor of Law
University of Idaho College of Law

Danielle Keats Citron
Lois K. Macht Research Professor &
Professor of Law
University of Maryland School of Law

Andrew Chin
Associate Professor of Law
University of North Carolina – Chapel Hill
School of Law

Sherry F. Colb
Professor of Law &
Charles Evans Hughes Scholar
Cornell Law School

Anthony Dillof
Associate Professor
Wayne State University Law School

David Gray
Professor of Law
University of Maryland
Francis King Carey School of Law

James Grimmelmann
Professor of Law
University of Maryland
Francis King Carey School of Law

Catherine M. Grosso
Associate Professor of Law
Michigan State University College of Law

Woodrow Hartzog
Associate Professor
Cumberland School of Law
Samford University

Andrew Jurs
Professor of Law
Drake University Law School

Margot E. Kaminski
Assistant Professor of Law
The Ohio State University
Moritz College of Law
Affiliated Fellow
Yale Information Society Project

Irina D. Manta
Assistant Professor of Law and Director of the
Center for Intellectual Property Law
Maurice A. Deane School of Law
At Hofstra University

Joseph Margulies
Professor of Law and Associate Professor
Visiting Professor of Government
Cornell University

William McGeveran
Associate Professor
Solly Robins Distinguished Research Scholar
University of Minnesota Law School

Steven John Mulroy
Associate Dean for Academic Affairs and
Professor of Law
Cecil C. Humphreys School of Law
University of Memphis

Paul Ohm
Professor of Law
Georgetown University Law Center

Neil M. Richards
Professor of Law
Washington University School of Law

Adina Schwartz
Professor, Department of Law, Police Science and Criminal Justice Administration
Assistant Director, Cybercrime Studies Center
John Jay College of Criminal Justice,
City University of New York (CUNY)

Robert H. Sloan
Professor and Head
Department of Computer Science
University of Illinois at Chicago

Christopher Slobogin
Milton R. Underwood Chair in Law
Professor of Psychiatry
Director, Criminal Justice Program
Vanderbilt University Law School

Stephen F. Smith
Professor of Law
University of Notre Dame
Eck Hall of Law

Katherine J. Strandburg
Alfred B. Engelberg Professor of Business Law
New York University School of Law

David Thaw
Assistant Professor of Law and Information Sciences
University of Pittsburgh
Affiliated Fellow
Yale Information Society Project