

The Times They Are a-Changin’ Regulating Collecting, Storing, and Sharing of Information

The Digital Revolution or the Third Industrial Revolution describes the period beginning in the 1980s when the world transitioned from a manufacturing-based economy to a service-based economy. The upheaval of the time changed our analog and mechanical devices to electrical, brought the personal computer, and the internet. This led to understanding the economy as the New Economy.

This Third Industrial Age is ongoing and in many ways the economy is still the New Economy. And now the next chapter is upon us—half of everyone on the planet uses the internet and 5 billion people subscribe to mobile phones. We are still not sure what to call the incoming era—the Sharing Economy, the Gig Economy, the Fourth Industrial Revolution, or Industry 4.0—but it is *happening*.

The domestic peer-to-peer based activity of providing goods and services is expected to grow from the early 2014 figure of \$14 billion to \$335 billion by 2025. This economic platform offers incredible flexibility, low entry barriers for workers, and increased efficiency. People can drive for Uber or Lyft as necessary to supplement their incomes.

The Gig Economy of freelance workers is estimated to be one-third of the U.S. workforce in 2017. By 2020 this number is expected to be in excess of 40%.

Existing companies will be innovating in the new era too. Thus, the policies formed in response to these changes will have an impact on the future ability to innovate across all sectors—digital or analog. Even technologies that do develop may do so more slowly or less effectively because of policy choices made years earlier.

Every Company Is a Data Company

In the current business landscape, collecting and using data is part and parcel with doing business. A business’s competitive advantage may be in its so called “Big Data”—the nuances of what sources of data it uses and doesn’t use, how it uses it, what the models are, what inferences and assumptions the business draws from the data, and what the conclusions are.

The term “Big Data” worked its way into the business and technology lexicon in the 1990s. The term describes the analytic ability of modern computing that allows unprecedented insight for businesses. The underpinnings of Big Data are the three Vs:

- **Volume:** aggregating entire streams of data from traditional and nontraditional sources on a large scale that would have been unthinkable in the analog era;

- **Velocity:** receiving and processing the information at high speeds nearing real time;

- **Variety:** formats that include traditional databases but also video, email and text documents.

Emerging technologies, such as the peer-to-peer provision of services, may offer novel uses and solutions, but the prevalence of businesses using data cuts across all industry lines. Accordingly, regulating the collection, storage, and sharing of information may affect the development of these technologies, but it will also have an impact on existing industries and business models.

Current Landscape of Business Regulation

Since the emergence of the Digital Revolution, the use of consumer data has been regulated largely in a uniform manner across all industries. The Federal Trade Commission’s (FTC) 2012 Privacy Framework reflected this approach and is applied to all commercial entities that collect or use consumer data. The FTC’s Framework reflected the general policy that has governed in the internet age: companies should be transparent about their data practices, companies should obtain affirmative consent before using consumer data in a way that was different than explained when it was collected or when the company is using sensitive data for certain purposes.

The FTC has found that more burdensome privacy regulations do not always benefit the consumer. Instead, the regulations are most efficient when they align with consumer preferences. Consumers’ preferences consistently show that their priority is focused on sensitive data, such as financial and health information, and information concerning children. Thus, the FTC instructed companies to obtain opt-in consent for this subset of consumer information. The FTC found, however, that this burden was unnecessary for consumer information which was used for commonly accepted practices such as fulfilling a consumer’s purchase of a product or service, preventing fraud, or marketing to the consumer.

This paradigm of technology and industry-neutral regulations on the collection, storage, and sharing of information has guided businesses to the cusp of the next economic era. The focus has been largely on the sensitivity of the information and not simply whether the data could at some point be linked to a consumer’s identity.

Recent action at the federal level has solidified that the Obama era FTC approach from 2012 will remain in place for

Expanding Opportunity An Agenda for All Californians

2018 Business Issues and Legislative Guide

See the entire CalChamber 2018 Business Issues and Legislative Guide at
www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsors
Of the 2018 Business Issues and Legislative Guide

Premier



Silver



Bronze



Iron



We're always with you.®

The Manatt logo consists of the word "manatt" in a white, lowercase, sans-serif font, centered within a solid yellow rectangular background.

the current administration. Some states, however, have proposed industry-specific regulations and a shift of focus from sensitive information to personally identifiable information. In 2017, a California Assembly bill, AB 375 (Chau; D-Monterey Park), proposed to create specific regulations focused only on providers of broadband internet. The bill also departed from the FTC approach by requiring opt-in consent for some nonsensitive customer information. This bill will be eligible for further consideration in 2018.

A currently pending California initiative, The Consumer Right to Privacy Act of 2018, also shifts away from the long-standing focus on sensitive information. Instead, the proposal contains significant restrictions on business use of any personally identifiable information. It couples these limitations with prescriptive regulations that businesses have to follow when collecting or sharing any Californians' information, and with a new regime of civil liability. The measure has been cleared to be circulated by its proponents for signatures, but has not yet qualified for the November 2018 ballot.

The California legislation and initiative are two of many challenges to the longstanding principles that have governed business collection, storage, and sharing of information.

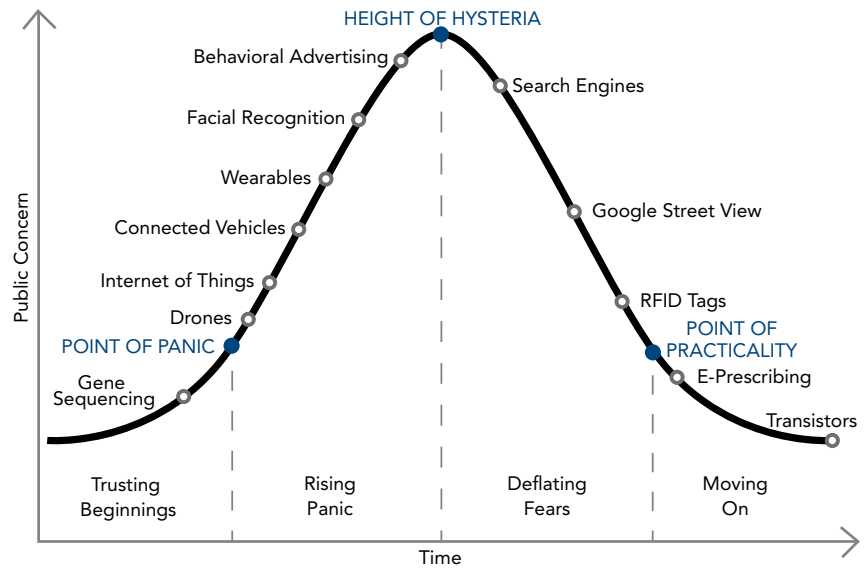
Government Use of Data

Evaluating the landscape of information regulation would be incomplete without considering government use of data. The state and federal governments hold massive amounts of information. In years past, the U.S. government had difficulty even identifying all its data centers. Many federal agencies have petabytes of information overwhelming their storage resources. After a long process, the federal government was able to identify and close more than 4,300 of 11,000 data centers, resulting in billions of savings.

The State of California also maintains vast quantities of information. In 2016 alone, the state had 30 security breaches that involved personally identifiable information. There are continuing policy decisions to be made about how state and local governments store and share this data. Many California proposals regulating use of information completely exempt public entities. Some proposals would even have the government act affirmatively to distribute personal information.

Many policymakers who support more onerous regulations on business use of data do not hold the same view for government use of data. For instance, California requires that home care aides register with the state. The process requires the workers to supply the state with various sensitive, personally identifiable information. In 2017, AB 1513 (Kalra; D-San Jose)

The Privacy Panic Cycle For New Technologies



Source: Technology and Innovation Foundation (September 2015).

attempted to create a mechanism of giving labor organizations (unions) access to the registered workers' names, telephone numbers, and cellular telephone numbers. The bill ultimately was vetoed by the Governor. This proposal, however, shows that the focus was not on individual privacy.

Current regulations require that transportation networking companies, like Uber and Lyft, provide the California Public Utilities Commission (CPUC) with an incredible volume of confidential data that includes the time, date, and pickup point and destination of every ride. At the urging of many local governments, the CPUC is currently considering whether it should put all of the data on a website portal that could be shared with the public.

Government use of information poses an additional concern over business use all together—the government can obviate the intentions of the business-consumer relationship. When a company uses a customer's information, that relationship is built on a transaction involving some combination of goods, services, money, and data. This exchange is laid out in terms of service and policies governing the exchange. Both the business and the consumer conclude that the transaction is in their best interest.

Both AB 1513 and the CPUC's proposal are after-the-fact regulations where consumers' privacy would be sacrificed without upfront understanding. Thus, the government presents an externality that cannot be evaluated at the time of the bargain. Both these proposals underscore the inconsistency in the regulatory landscape, particularly when it comes to government directly controlling the information.

Emerging Technology—Policy for Policy's Sake

Regulating the sharing of information has a particularly deleterious

effect on innovation. The Information Technology and Innovation Foundation (ITIF) think tank has coined the phrase the “privacy panic cycle” to describe the fear that emerges upon introduction of new technology, grows rapidly, and eventually declines as the technology becomes commonplace and accepted. The infographic on the previous page represents how ITIF saw the cycle in 2015.

The cycle also can repeat upon the introduction of new iterations of technology. The Kodak camera was invented in 1888. Over the next 10 years it started to become mainstream. The panic grew about the new technology and a term was coined for the “Kodak Fiend”—those who dared take pictures in public. Newspapers of the day decried the effects on society.

“One of the nuisances of our civilization is the man or the woman who goes about armed with a kodak and snapping at everybody who passes or who can be espied. There seems to be something in the kodak which destroys all sense of propriety in its average possessor. As soon as he owns or hires one of these instruments the ordinary individual often becomes oblivious to the canons of decency, sticks his nose into matters with which he properly has no business—and tries the patience of polite persons almost beyond endurance.”

— *Los Angeles Herald*, Number 311 (August 7, 1899).

But is it so different from today? The cycle is repeating itself with the rise of smartphones and social media.

“Welcome to the runaway converge of cameras, social media, and platforms that range from a person’s eyes, skin and clothing, to toothbrushes, jewelry, shirt buttons, soda cans, teddy bears.”

“The U.S. has become a ‘shoot and share’ society that’s flooding social media with content that’s alternately sublime, endearing, trivial, violent, and an assault on privacy and civility.”

— *San Diego Tribune*, “Say hello to the camera, goodbye to privacy” (February 3, 2017).

As the public level of panic hits a crescendo, policymakers react. Often the novel technology does not require a novel solution. Governor Edmund G. Brown Jr. has recognized this policymaking tendency. In vetoing bills criminalizing operation of drones over prisons or in a manner interfering with firefighting, he stated:

“Each of these bills creates a new crime—usually by finding a novel way to characterize and criminalize conduct that is already proscribed. This multiplication and particularization of criminal behavior creates increasing complexity without commensurate benefit.”

— Governor’s Veto Message on AB 168 (Gaines; R-El Dorado Hills and Jackson; D-Santa Barbara; 2015) and AB 170 (Gaines; R-El Dorado Hills; 2015).

Instead of focusing on the urge to regulate the new technology, Governor Brown directed policymakers to focus on the actual issue presented by the technology. Does this technology present a new issue that demands a new law? Is there a real harm that needs to be addressed? Such a focus also helps moderate the effects of the privacy panic cycle.

CalChamber Position

The Digital Revolution developed because the great minds of Silicon Valley were able to develop the internet without being weighed down by prescriptive regulations. The United States should seek to retain its place as the norm setter for what technologies are adopted and how they are regulated. Doing so would have deep implications for the long-term health of the country. However, the United States’ place on top is not guaranteed. California was a critical player in the Digital Revolution, but now sits in a precarious position of out-regulating itself from the next wave.

The times are always a-changin’. And that is not reason enough for new regulations.



Staff Contact
Kevin McKinley
Policy Advocate

kevin.mckinley@calchamber.com
January 2018