Background Paper for the Assembly's Informational Hearing on Digital Privacy

"Brave New World: The Collecting, Sharing and Tracking of Personal Information On-Line and in the Mobile App Ecosystem"

I. INTRODUCTION

California has been at the forefront of both innovation and privacy protection. The recent *Apple v Superior Court of Los Angeles County (Krescent)*[1] decision this past month highlights the need for California privacy law to be updated from the "brick and mortar" world to an online world reflective of new business models that foster innovation while providing access to free content and services. As this paper will note, lawmakers will have to strike the right balance between a robust and innovative internet and one that adequately protects individual privacy. This is clearly not an easy task, but it is a critically-important one.

In beginning to answer that call, this paper represents only some initial comments and information in what will continue to be a much larger conversation, not just here in California but across the country. So to guide that discussion in the most productive direction possible, it is important to make clear the paper's scope: this paper aims to address information privacy *within the context of Personally Identifiable Information (PII) and the online world*.

To that end, it focuses on the different state, federal and international laws that protect PII retained and transmitted in an electronic format. Electronic commerce is naturally a central part of that discussion, but we are not necessarily restricted to that area alone. Future legislative hearings will explore specific privacy issues in greater detail. With that, we begin with an overview of privacy and consumer protection and then explore the impact of limitations on innovation in the new economy.

A. WHAT DO THEY KNOW, HOW DID THEY GET IT, AND HOW SECURE IS IT?

In a now classic 1890 *Harvard Law Review* article entitled "The Right to Privacy," Louis Brandeis and Samuel Warren argued that the law needed to evolve in order to respond to technological changes. The technological changes that most concerned them were simultaneous advances in documentary photography and mass-circulation newspapers. Recent advances in photography meant that photographs could be taken of people in public places, without their knowledge or consent. Combined with the advent of cheap, mass-circulation newspapers, these unauthorized photographs – often published along with salacious details about the subject – could be widely, and profitably, distributed. Brandeis and Warren wrote:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' [T]he question

> whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.[2]

Fast forward more than 120 years and, once again, we find ample evidence on a daily basis why we again need to consider how the law needs to evolve to respond to the technological advances in this new "Information Age." Policy-makers are increasingly confronted with the question: Is technology putting our privacy, finances, and even our safety at risk? Recent news reports highlighted that First Lady Michelle Obama was the latest public figure to have her Social Security number and credit report leaked online by a website posting private data on celebrities and government officials. Thus fears are increasingly expressed in the media and in statehouses across the country as to whether the Internet is too susceptible to breaches of private information, and whether consumers have any real understanding about what personal information of theirs is being shared with others.

Indeed, legal scholars, journalists, and other commentators are increasingly drawing policy-makers' attention at all levels of government to how new technologies and business methods are posing new threats to our privacy and taking advantage of consumers' lack of understanding about how data about them is collected and shared. In a 2010 series entitled, "What They Know," the *Wall Street Journal* (WSJ) published more than a dozen articles regarding on-line data gathering – according to WSJ, it is the fastest-growing business in America. The inaugural article found that "the nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning."[3] This tracking technology – often referred to as "cookies" – consist of small files that are downloaded onto the user's browser and have the capacity to track subsequent websites visited by that user. While users of these websites may voluntarily disclose personal information to use the websites they actually visit or when they purchase goods online, the series noted, they often do not know that the majority of those websites permitted third parties, including advertising networks, to install cookies on the user's computer.

This exposes a major paradox about the Internet today: that the gathering of anonymous data about Internet users' preferences and habits is a critical building block supporting the modern Web as we all know and take advantage of it. Yet it is that very need for data collection and monitoring that, without adequate controls and oversight, may inadvertently subject millions of Internet users to the unwanted sharing of their personal information.

B. SOME OF THE KEY PUBLIC POLICY QUESTIONS FACING LAWMAKERS TODAY AS THEY STRIVE TO STRIKE THE RIGHT BALANCE BETWEEN A ROBUST AND INNOVATIVE INTERNET AND ONE THAT ADEQUATELY PROTECTS INDIVIDUAL PRIVACY

As part of its "What They Know" series, the *Wall Street Journal* published an exchange of editorials by Nicholas Carr, an author and privacy rights advocate, and Jim Harper, the director of information policy studies at the Cato Institute. Carr argued that the harvesting of our personal information without our knowledge, much less our consent, was nothing less than an "assault on liberty." In addition to the danger that our personal information will end up in the wrong hands, or that advertisers will manipulate us and our information in order "to influence our behavior and even our thoughts in ways that are

invisible to us," Carr saw an even greater danger: that "continuing erosion of personal privacy . . . may lead us as a society to devalue the concept of privacy, to see it as outdated and unimportant."[4]

In stark contrast, Jim Harper emphasized the many benefits that consumers gain from tracking and information sharing. It is not simply that targeted ads are more useful to us; more importantly, Harper contends, it provides users with more free online services: "The reason why a company like Google can spend millions and millions of dollars on free services like its search engine, Gmail, mapping tools, Google Groups, and more is because of online advertising that trades in personal information."[5]

When it comes to the collection, sharing, and tracking of personal information, these contrasting views go to the heart of the matter. As Harper notes, companies like Google and most other commercial websites make their money by selling advertisement space based on the user's profile or by permitting third parties to install cookies on their websites. Online services, like Google maps, cost money to produce and maintain, yet they are free to the user. Without the advertising revenue, Google and other companies would need to charge a user fee. Some sites – for example, the popular Ancestry.com – charge users a monthly fee.

Given the advertising-driven business model of the commercial Internet, can we formulate policies that strike a balance between providing consumers with the kinds of online services that they apparently hunger for, while at the same time protecting a consumer's right to privacy? Is it the responsibility of each consumer to strike that balance for himself or herself? Can consumers reasonably strike that balance if they lack adequate information about the kinds of information that is tracked and with whom it is shared? Can they strike that balance if they do not have adequate control over third party use of their personal information?

One of the underlying policy questions in the debate over online tracking and behavioral advertising concerns the extent to which privacy protections should come from industry self-regulation or government-mandated regulation. According to a recent report by the *Washington Post*, browser manufacturers – including Google, Apple, Microsoft, and Mozilla – are considering browser controls that would limit the ability of third party advertisers to install tracking cookies on a user's computer browser. At present, some browser manufacturers, including Microsoft, have implemented privacy controls in its latest Internet Explorer that allow a user to transmit a "request" not to track their behavior across websites. However, neither existing controls or options, nor existing law, requires an advertising network or commercial website to *honor* those requests. According to the *Post* report, the new devices under consideration would not simply send a request but actually *block* cookies. Just what the effect of this development will be is uncertain. Some privacy groups applaud the idea as a meaningful control. Other privacy advocates contend that it will lead to an "arms race" as the advertising industry develops new technologies that counter the new controls. Some advertisers, on the other hand, contend that this will destroy the Internet by undermining the business model that provides users with free online services.[6]

The dilemmas created by more advanced technology go beyond consumer privacy and behavioral advertising, however. For example, new digital technology allows health care professionals to instantly share medical records in ways never before possible. This not only has the potential to improve health care delivery, potentially save lives; and it has the power to lower administrative costs. The digitization of medical records allows consumers to construct their own "personal health records", allowing them to

become more involved in and to take greater control over their own health and health care. On the other hand, medical information can be a particularly sensitive piece of personal information, and in the wrong hands it could be used to deny a person employment or health care coverage, or even to harass or blackmail. Once again we see how new technology creates both extraordinary benefits while at the same time posing potentially serious threats to privacy. Can we protect privacy without undermining those benefits?

Finally, new technology creates new opportunities for surveillance, both by governmental and private actors. In the coming months, policy committees, and the Legislature as a whole, will consider an unprecedented number and breadth of privacy-related bills. In doing so, an understanding of the evolving case law surrounding privacy, technological innovations, differing business models as well as the principal constitutional and statutory provisions, will be needed. Following is a discussion of that legal framework.

II. LEGAL BACKDROP: GENERAL PRIVACY PRINCIPLES AND CONSTITUTIONAL PROTECTIONS

The Right to Privacy Under the United States and California Constitutions: The United States Constitution does not *expressly* provide a right to privacy. Yet historians, legal scholars, and the courts have widely construed the Bill of Rights and the liberty clause of the 14th Amendment to provide several *implicit* protections of privacy. For example, the First Amendment protects the privacy of beliefs; the Third Amendment protects the privacy of the home from the forced quartering of troops; the Fourth amendment protects our person and possessions from unreasonable searches; and the Fifth Amendment protects us from being compelled to reveal self-incriminating information. In addition, the Ninth Amendment states that the "enumeration of certain rights" in the Bill of Rights "shall not be construed to deny or disparage other rights retained by the people," making clear that other traditionally recognized rights are protected even if they are not expressly mentioned. (*Griswold v. Connecticut* (1965).) As Justice Louis Brandeis argued, one of these traditional, unenumerated rights is the right to privacy. This right to privacy – or the "right to be left alone" – was, according to Justice Brandeis, "the most comprehensive of rights and the right most valued by civilized men." (*Olmstead v. U.S.* (1928)).

The California Constitution, unlike the U.S. Constitution, *does* expressly protect an individual's right to privacy. Added to the California Constitution in 1972 when voters adopted Proposition 11, the California privacy provision differs from the federal constitution in another important respect: it protects an individual's right to privacy from *both* governmental and private actors, while the federal constitution only applies to governmental actors. (*Hill v. National Collegiate Athletic Association* (1994) 7 Cal. 4th 1.)

The California Supreme Court has held that the privacy provision in the California Constitution "creates a legal and enforceable right of privacy for every Californian." (*White v. Davis* (1975) 13 Cal. 3d 757, 775.) Despite this express protection, however, just what is included in the state's constitutional right of privacy has necessarily been developed in a body of case law. These cases tend to be very fact-specific. As a general rule, however, in order to maintain a claim for infringement of one's right of privacy under the California Constitution, the plaintiff must (1) identify a legally protected privacy interest; (2) establish that he or she had a "reasonable expectation of privacy" under the circumstances; and (3) that the defendant's conduct constituted a "serious" invasion of privacy. If a plaintiff establishes all three of

these elements, the defendant may still show the invasion of privacy was justified if it furthers a legitimate and competing interest. Specifically, the California Supreme Court has held that an "[i]nvasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest." (*Hill*, supra at 39-40.)

In addition to these broad constitutional principles, California law also imposes both civil and criminal liability for invasions of privacy. Under common law tort principles, state law imposes civil liability for four kinds of invasion of privacy: (1) Intrusion upon the plaintiff's seclusion or solitude or into his or her private affairs; (2) Public disclosure of private facts about the individual; (3) Publicity that places the plaintiff in a false light in the public eye; and (4) Misappropriation, for the defendant's advantage, of a person's name or likeness. (5 Witkin, Summary of Cal. Law (10^{th} ed.) Torts, Section 651.) State law also creates criminal liability for certain invasions of privacy in Penal Code Section 630 *et seq.* These statutes provide criminal penalties for certain kinds of conduct, including unauthorized wiretapping, electronic eavesdropping, intercepting cellular phone communications, and electronic tracking of individuals, except as specified.

The "Reasonable Expectation of Privacy:" Whether one is evaluating the right of privacy under the California or the U.S. Constitution, or assessing civil or criminal liability for an "invasion of privacy," a core consideration is whether the person alleging the violation has a "reasonable expectation of privacy" under the circumstances. (*U.S. v. Katz; Hill*, supra.) In *Katz*, the U.S. Supreme Court held that a person is not protected by the Fourth Amendment unless that person can show that he or she had a reasonable expectation of privacy in the place that was searched or the property that was seized. The Court reasoned that what "a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection…. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (*Katz v. United States* (1967) 389 U.S. 347.)

Although originating in the context of Fourth Amendment law, the concept of a "reasonable expectation of privacy" has generally migrated to other areas of privacy law. For example, the civil tort of intrusion generally requires an intentional intrusion "into an arena where one reasonably expects privacy." As a general rule, the "reasonable expectation of privacy" does not extend to things or to information that has already been knowingly exposed to the public.

This does not mean that all actions that take place in a public space are not protected. The key issue is whether the person reasonably expected that what was intruded upon would remain private. For example, in *Katz* the criminal defendant was making a call from a public telephone booth. Even though the defendant was in a public place and could be seen through the glass of the telephone booth, he had a reasonable expectation of privacy in the content of his telephone conversation once he closed the phone booth door. One of the most interesting questions facing courts and lawmakers today is how to apply this concept in the age of the Internet and social media. For example, one could argue that Facebook or other social media postings are, almost by definition, made public – at least to a certain number of people. On the other hand, one could also strongly argue that if a person deliberately set his or her privacy settings so that only a select group of friends could see the posting, then the person might have a reasonable expectation that other people would not see it.

A 2009 California appellate court held that posting information on a social networking site may extinguish any reasonable expectation of privacy. In *Moreno v. Hanford Sentinel* (2009 Cal. App. LEXIS 472), a California appeals court held that once an image or other information has been posted on an Internet web site, it is no longer a "private" fact that can be protected from public disclosure. The court noted that a critical element of the constitutional right to privacy under the California constitution is a "reasonable expectation of privacy," and that when a person posts information on an Internet web site they lose any reasonable expectation of privacy. Similarly, a tort action requires public disclosure of a "private fact," but the court similarly concluded that a fact is no longer "private" when it has been voluntarily posted on the Internet – even if it was on a network with limited access, since it was posted to numerous people and was no longer "private" in any meaningful legal sense.

Even if one accepts the court's opinion that one does not have a reasonable expectation of privacy in something that was knowingly broadcast to others by posting it on the Internet or social media site, one could still argue that a person has a reasonable expectation that his or her online behavior – websites visited or things purchased online – will not be tracked and aggregated by third party cookies, especially when the person is not notified that those cookies have been installed. In short, if one posts a photograph on a website there may no longer be a reasonable expectation of privacy in that photograph; but there may be a reasonable expectation after leaving the website that subsequent online behavior will not tracked by an unknown third party that planted a cookie on the computer while visiting the first website. It is to this issue that we next turn.

III. ONLINE AND MOBILE PRIVACY: COLLECTING, SHARING, AND TRACKING PERSONALLY IDENTIFIABLE INFORMATION (PII)

As noted above, the *Wall Street Journal* digital privacy series placed in question the extent to which personal information is collected and shared on the Internet. Indeed, this collecting and selling of personal information for purposes of targeted advertising drives the Internet economy, and as many note, even makes it possible. Indeed, the only reason many Internet and online services are free to the using public is precisely because the cost of keeping those websites operative and providing the online service is paid for by advertisers.

While the collecting and sharing of personal information, including the tracking of online behavior, has thus been an integral and foundational part of the Internet economy, the recent proliferation of mobile applications (or "apps") has raised many new privacy questions and concerns. Two aspects of the so-called "mobile app ecosystem" are particularly noteworthy.

First, by their very nature, mobile apps not only allow data brokers and advertising networks to track a user's online behavior, they also allow them to link this behavior with the user's physical location.

Second, the mobile app ecosystem involves a remarkable multiplicity of players: application developers, application "platforms," advertising networks, credit card payment processors, mobile service carriers, and data brokers who aggregate and resell information from a variety of sources, just to name a few. The multiplicity of players creates special problems. For example, as between the app developer and the app platform, which party should be responsible for complying with laws and regulations governing disclosure and the posting of privacy policies? This section examines existing state and federal laws, as

well as policy guidelines, relating to the collecting, sharing, and tracking of personally identifiable information (PII), including the applicability of these laws and guidelines in the new mobile ecosystem.

As we have seen, privacy is not a question of first impression; it is a matter of long-standing concern for the law at every level of government. In recent years, governments at state, federal and even international levels have sought to make strides in setting out rules and guidelines for protecting the privacy of our information from a myriad of threats. However, as technological advances continue to create ever greater amounts of information with greater freedom of movement, the information itself becomes more valuable to us and to others – and that increasing importance is what makes individuals feel so vulnerable to its misuse.

The kinds of information that the law now endeavors to protect takes many forms; personally identifiable information (PII) can be personal (relating to one's identity), financial, health-related, behavioral, and even geospatial. The uses of "PII" are also many - personal information can be shared to communicate with family and friends, to facilitate commerce, to better manage our own health, to participate in government programs, to use technology and the Internet more efficiently, and even to enforce the law. Of course, PII can also be sought after for less socially positive reasons, such as consumer profiling, unwanted direct and third party marketing and even identity theft or fraud.

Correspondingly, there are different frameworks and existing laws to protect that information, and this next section will summarize some of those approaches. But just as the forms of PII and the technologies we use to collect and communicate it naturally evolve, so to must the law, lest the tools we create outpace the rules designed to protect us from their misuse. Nowhere is this more important than in the fields of electronic commerce and mobile communications.

The recent *Apple v Superior Court of Los Angeles County (Krescent)*[7] decision from February 2013, discussed in greater detail below, is a case in point. In *Apple*, the California Supreme Court opined that the state's statutory protection against the collection of PII when making credit card purchases does not apply to online retailers of electronically downloadable products. The underlying statute, the Song Beverly Credit Card Act passed in 1990, generally prohibits businesses from requesting or requiring consumers to provide unnecessary PII during a credit card transaction. However, the *Apple* Court found, in essence, that the statute and its anti-fraud provisions had been designed for "brick and mortar" transactions that pre-dated the Internet era and the explosion of e-commerce, and that online retailers of electronically downloadable products were therefore outside of the intended scope of the law. Of course, the Court also recognized the problem of new technologies outpacing existing laws, and the majority opinion explicitly invited the state Legislature to revisit the matter, and update its consumer protection laws accordingly should it so desire.

This section will review key state and federal laws related to data collection, use and retention, as well as tools to permit meaningful consumer control of PII and limits on government. We begin with an overview of two overarching frameworks, a new federal framework from the Obama Administration and the existing European Union privacy directive, to guide our thinking about how to regulate online privacy carefully yet effectively. We will conclude with a larger discussion of the *Apple* case, and the implications for existing law raised by new mobile technologies and the burgeoning "app ecosystem."

The White House Consumer Data Privacy Framework: The White House Consumer Data Privacy Framework (hereinafter, "Framework"), released by the Obama Administration last year in February 2012, represents a comprehensive, high-level approach to providing consumer privacy protections while still promoting innovation.[8] The Framework contains four major elements: the Consumer Privacy Bill of Rights (CPBR), a multi-stakeholder process to operationalize the CPBR in different business contexts, an effective enforcement plan, and a commitment to increased interoperability with existing international privacy regimes.

The first element, the CPBR, is intended to provide "a baseline of clear protections for consumers and greater certainty for companies."[9] It contains seven comprehensive, globally recognized "Fair Information Practice Principles" (FIPPs) to guide the development of codes of conduct for stakeholder companies and others that would be enforceable through federal legislation. As a set of general principles, the CPBR is designed to give companies and industries enough flexibility to implement the framework within their own unique context without slowing innovation. It also allows those companies to focus on those privacy matters of greatest concern to their own customers and stakeholders without a one-size-fits-all mandate. Those seven principles are:[10]

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The second element, fostering a multi-stakeholder process to develop enforceable codes of conduct, is intended to lead to enforceable codes of conduct that implement the CPBR.[11] That process would require government to bring together stakeholders within differing market segments – including consumer groups and privacy advocates – to develop industry-specific codes of conduct. While stakeholders need not participate, and individual companies need not adopt the resulting code for their industry, codes of conduct would be legally enforceable. Major benefits of this approach include the fact that it is informed by the technical knowledge of the companies themselves, and that it provides some consistency across companies which will be less confusing for consumers.[12]

The third element of the Framework is stronger enforcement.[13] In the federal context, the Federal Trade Commission and state Attorneys General would be given greater authority to enforce the CPBR and adopted codes of conduct. Enforcement is viewed as critical to ensuring that companies are held accountable for their statements to consumers relating to privacy, and also helps to prevent an uneven playing field between competitors.

The fourth and final element is greater coordination with existing privacy frameworks in other countries.[14] By harmonizing with the EU Data Privacy Directive and other international privacy regimes, the Framework would achieve increased international interoperability with consistent, low-barrier rules in a decentralized landscape. This interoperability element is underpinned by the subprinciples of 'mutual recognition'[15] and 'enforcement cooperation'[16], which suggest an approach that will be both comprehensible to and enforceable by other nations.

The U.S. Department of Commerce's National Telecommunications and Information Administration convened its first privacy multi-stakeholder meeting on July 12, 2012.[17] The topic of the first meeting was the development of codes of conduct for the handling of personal data by providers of applications and interactive services for mobile devices. Additional stakeholder meetings on mobile application transparency will be taking place from January through April of 2013.[18]

European Union Data Privacy Directive & Draft Data Protection Regulation: Originally passed in 1996, the European Union (EU) Data Privacy Directive (Directive 95/46/EC) (hereinafter, the "Directive") generally requires EU member states to enact their own national data protection laws reaching both governmental and private entities, including businesses that process employee and consumer data, in harmony with the principles laid out in the Directive. On January 25, 2012, the European Commission released a draft European General Data Protection Regulation (the "Proposed Regulation") that would supersede the current Directive.[19]

At the philosophical level, the EU treats privacy as a component of human rights, with all EU members being signatory to the European Convention of Human Rights which recognizes a right to respect for one's private and family life, home and correspondence, subject to certain restrictions.[20]

The Directive generally prohibits all "processing" of "personal data" except that which is fair, lawful and legitimate.[21] As a basic matter, personal data must be treated with transparency, legitimacy and proportionality. This means that personal data must be processed fairly and lawfully; collected for specified, explicit and legitimate purposes without further processing; adequate, relevant and not excessive in relation to the original purpose for collection; accurate and kept up-to-date; and kept for no longer than necessary for their original purpose.[22] Furthermore, personal data may only be processed if the data subject has unambiguously granted his or her consent; when necessary for a contract; when necessary to meet a legal obligation by the controller; to protect the vital interests of the data subject; when necessary to carry out a task in the public interest; and where the legitimate interests of the controller or other third party are disclosed.[23]

The data subject enjoys the right to be informed when his or her data is collected, including the identity of the controller or its representative; the purpose of the processing; the recipients of the data; and any other information required, as specified.[24]

Each EU member must create a "supervisory authority" to administer and enforce the Directive. Aggrieved individuals can file complaints with the authority[25], and controllers must notify the authority when processing personal data (including the purpose of the processing, categories of affected data, recipients of data, proposed transfers, and a description of security measures taken.[26] Data may be transferred outside of the EU only if the recipient country offers "an adequate level of protection."[27]

Privacy Law Overview: Key Federal Statutes

Health Insurance Portability and Accountability Act of 1996 (HIPAA): The Health Insurance Portability and Accountability Act is a federal law that was enacted in 1996. Its privacy regulations protect patients' privacy by limiting the ways that health plans, pharmacies, hospitals and other covered entities can use patients' personal medical information. The regulations protect medical records and other individually identifiable health information, whether it is on paper, digital or communicated orally.

A covered entity may disclose PHI (Protected Health Information) to facilitate treatment, payment, or health care operations without a patient's express written authorization. Any other disclosures of PHI (Protected Health Information) require the covered entity to obtain written authorization from the individual for the disclosure. However, when a covered entity discloses any PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose.

HIPAA gives individuals the right to request that a covered entity correct any inaccurate PHI. It also requires covered entities to take reasonable steps to ensure the confidentiality of communications with individuals. HIPAA also requires covered entities to notify individuals of uses of their PHI. Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures.

Gramm-Leach-Bliley Act (GLB): The Gramm-Leach-Bliley Act is a federal law that was enacted in 1999. The law requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. Whether a financial institution discloses non-public information or not, they must have a policy in place to protect the information from foreseeable threats in security and data integrity. Three main components of the law are the financial privacy rule, the safeguards rule, and the pretext rule.

The financial privacy rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The safeguards rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. The pretext rule encourages organizations to implement safeguards against pretexting. Pretexting occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder by phone, by mail, by email, or by "phishing" (i.e., using a phony website or email to collect data).

Privacy Law Overview: Key California State Statutes

Song-Beverly Credit Card Act of 1971: Under state law, a person who accepts a credit card for payment shall not record the consumer's personal identification information on the credit card transaction form, except as specified. Originally enacted in 1971, the Song-Beverly Credit Card Act (Civil Code Section 1747.01 *et seq.*) regulates the issuance and use of credit cards and the respective rights and responsibilities of cardholders and retailers. Section 1747.08 of the Act, in particular, seeks to protect a consumer's privacy and to address the "the misuse of personal identification information for, inter alia, marketing purposes." (*Absher v. Autozone, Inc.* (2008) 164 Cal. App. 4th 332, 345.) Specifically, the Act prohibits a retailer from requesting, as a condition of acceptance of a credit card, that the cardholder

provide the retailer with "personal identification information," which is defined to mean any information about the cardholder that does not appear on the card, including, but not limited to, the cardholder's name and address.

Existing law carves out reasonable exceptions to this general rule, including where the business is contractually or legally required to collect the information, or where the business needs the information to perform some "special purpose," such as shipping, installing, or servicing a purchased item. A business that accepts credit cards is also permitted to require the cardholder, as a condition to accepting the card as payment, to provide reasonable forms of identification, such as a driver's license. Last year's AB 1219 created another limited exception: in order to prevent fraud, a business that sells fuel may ask the purchaser to provide a zip code in order to process a fuel purchase at an automated fuel dispenser island. A person or business that violates the Act is subject to civil penalties, which may be assessed in a civil action by an affected cardholder, or in an action brought by the Attorney General or a district or city attorney. As discussed at greater length below, the California Supreme Court held earlier this year that the Song-Beverly restrictions relating the collection of personal information during a credit card transaction do not apply to online credit card purchases.

California Medical Information Act (CMIA): The California Medical Information Act was codified in 1981 in the California Civil Code at Section 56.10, *et seq*. It protects an individual's medical information by limiting situations where a health care provider may share the information. The law states that "no provider of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization." In addition to any other remedy at law, any patient whose information has been disclosed in violation of this law may recover compensatory damages, punitive damages not to exceed $3,000, attorney's fees not exceed $1000, and the costs of the litigation. (Civil Code Section 56.35.) There are exceptions to the law where a health care provider can share personal medical information without authorization from the patient. These exceptions permit a provider to share information with other healthcare providers to facilitate diagnosis and treatment, to find financially liable party and obtain payment, with administrative subcontractors, with quality control organizations (peer review boards, etc.), with accrediting agencies, with coroners, and for bona fide research purposes.

Government Code 11019.9: Government Code 11019.9 is a section codified in California law that states "Each state department and state agency shall enact and maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977" (California Civil Code, Sections 1798 *et seq*).

The privacy policy a state department or agency maintains must include the following principles: personally identifiable information is only obtained through lawful means, the purposes for which personally identifiable data are collected are specified at or prior to the time of collection, and any subsequent use is limited to the fulfillment of purposes not inconsistent with those purposes previously specified. A state department or agency must also not disclose personal data for purposes other than those specified, except with the consent of the subject of the data, or as authorized by law or regulation. Additionally, personal data collected must be relevant to the purpose for which it is collected and the general means by which personal data is protected against loss must be posted.

Information Practices Act of 1977 (IPA): The Information Practices Act of 1977 is a codified in the California Civil Code, Section 1798, *et seq*. It requires state agencies to protect personal information

they maintain. Information protected by the IPA includes any data that describes or identifies a person, including the person's name, address, phone number, Social Security number, and medical, employment and education history. State agencies are required under the IPA to collect only information that is relevant to the purpose of the agency and to obtain that information from the individual, rather than a secondhand source, if possible. The agencies are required to keep records of the information they collect and to store the original sources of the information.

In order to share the information it has collected, the state agency must have the permission of the individual or demonstrate the necessity of disclosing the information. Information can be shared if it is necessary to a function of another agency, such as enforcing the law. The IPA allows an individual to examine records about the individual that state agencies maintain. The individual can petition the agency to correct or remove information that is erroneous or irrelevant. A person may file a civil lawsuit against an agency that doesn't maintain information in accordance with the law or refuses to provide records. A person who illegally obtains or misuses an individual's personal information may be charged with a misdemeanor.

California Online Privacy Protection Act (Cal OPPA): The California Online Privacy Protection Act of 2003 (Cal OPPA) is a California State Law codified into the California Business and Professions Code Section 22575 *et seq*. It states that operators of commercial websites that collect personally identifiable information from California's residents are required to conspicuously post and comply with a privacy policy that meets certain requirements. The privacy policy must identify the categories of personally identifiable information that the operator collects about individual consumers and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

If the operator maintains a process for an individual consumer to review and request changes to personally identifiable information that is collected through the Web site or online service, it must provide a description of that process. The operator must also describe the process by which it notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy. The privacy policy must also identify its effective date.

"Shine the Light" Law: California's Shine the Light law is codified in the California Civil Code Section 1798.83. It is a privacy law passed by the California State Legislature in 2003. It addresses the practice of sharing customers' personal information for marketing purposes, also known as list brokerage. The law outlines procedures requiring companies to disclose upon the request of a California resident what personal information has been shared with third parties, as well as the parties with which the information has been shared. The law also outlines specific language that companies who do business with California residents must include in their online privacy policies.

The law requires that a business establish a designated contact point where they may direct Information-Sharing Disclosure requests. In addition, a business must do at least one of the following: sufficiently provide to all employees who may have contact with consumers the contact points, add a link on its Web site's home page titled "Your Privacy Rights" or "Your California Privacy Rights", or include one of those phrases in the same style as the heading "Privacy Policy" on a business's privacy policy page. That section or separate "Your Privacy Rights" page must describe a customer's rights as outlined by the law and provide information to the consumer regarding the designated contact point. The company must clearly post or make available the contact information everywhere a customer interacts with the business' employees in California.

Additionally, businesses must provide to the consumer a complete list of all personal information disclosed to third parties and the nature of that information within 30 days of the request

Recent Key Court Cases:

"Personal Identification Information" Under Song-Beverly -- *Pineda*: In 2011 the California Supreme Court confronted the question of what constitutes "personal identification information" under the Song-Beverly Credit Card Act and, more specifically, whether a person's zip code – with nothing else – constitutes an "address." (*Pineda v. Williams- Sonoma Stores, Inc.* (2011) 51 Cal. 4th. 524.) In *Pineda,* a customer sued a retailer claiming that it had violated the provisions of the Song-Beverly Act when a store clerk asked the customer for a zip code during the credit card transaction, and then recorded that zip code along with the customer's name and credit card number. The customer subsequently learned that the retailer used this information to do a "reverse search" to locate the customer's home address. The retailer then kept the customer's information in a data base that it used for marketing purposes. The customer filed the matter as a putative class action, alleging invasion of privacy, unfair competition, and violation of the Song-Beverly Act. Both the trial court and the Court of Appeal sided with the retailer, finding that a zip code, without any other component of the address, was too general to be considered "personal identification information." However the California Supreme Court reversed, holding, unanimously, that the word "address" in the statute means either a complete address or any portion of an address, and that a zip code is "readily understood to be part of an address." (*Id.* at 531.)

"The Recent *Apple* Case" -- Online Businesses Held Not to Be Covered by Song-Beverly: Earlier this year the California Supreme Court considered whether the provisions of the Song-Beverly Act prohibited the collection of personal information applied to online businesses. (*Apple v. Superior Court of Los Angeles (Krescent*).) A bare majority of four justices held that it did not apply to online businesses. The majority opinion conceded that the statute does not make any express exception for online business transactions – applying as it does to *any* person, firm, etc. that accepts credit cards. However, the court concluded that both the legislative history and the overall statutory framework strongly suggest that the statute was only meant to apply to in-person transactions at brick and mortar businesses; online purchasers were not contemplated.

In support of this conclusion, the Court made the following points:

- When the statute was originally enacted in 1971 the Internet did not exist, and even at the time of the most recent amendment – 1991 – online commercial sales were virtually non-existent and certainly not widespread, suggesting that the original intent of the legislature concerned in-person brick and mortar transactions.

- In order to prevent fraud, the statute permits a business to require the customer to present a form of identification, such as a driver's license or other photo ID, so long as none of the information is written down or recorded. This provision, the court reasoned, showed that the overall framework did not contemplate online transactions, for an online business would not be able to request a photo ID for purposes of fraud prevention.

- The California Online Privacy Protection Act (Cal OPPA, B&P Section 22575 *et seq*.), which expressly regulates commercial websites and online services, clearly anticipates that online business can and do collect personal information. Cal OPPA applies to any commercial website

or online service that collects personal information from consumers, including consumers who use the website or online service to purchase goods. Cal OPPA places no restrictions on the ability of these websites and online services to collect personal information; in fact, it assumes that they do collect that information and only requires that they post a privacy policy that tells consumers what types of personal information is collected and with whom it is shared.

Uncodified FTC Policy Guidance

In addition to statutory provisions dealing with various types of sensitive information, both the federal and state governments have issued policy guidelines for industry to follow. While they do not have the force of law, these guidelines do articulate important policy principles.

Federal Trade Commission guidelines: The Federal Trade Commission, a federal administrative agency that promotes consumer protection, has published several whitepapers on privacy. Below is a summary of two of the most recent and relevant white papers.

A. "Mobile Apps for Kids"

In 2012 the FTC issued "Mobile Apps for Kids." The report identified three key players in the kids app ecosystem: the app stores, developers, and third parties providing services within apps. Key findings include that most mobile apps for kids are collecting information from children including device IDs, phone numbers, locations, and other private information without their parents' knowledge or consent. The study stated nearly 60% of the mobile apps the FTC reviewed from the Google Play and Apple App stores transmitted the device ID. The apps also often shared that ID with an advertising network, analytics company or another third party. Of those 235 mobile apps, 14 also transmitted the location of the device and the phone number, the FTC found.

Among the recommendations the FTC made were suggestions to App developers to include simple and short privacy policies/disclosures formatted in a way that is appropriate for a small screen, and that they should alert parents if the app connects with social media or allows targeted advertising. The FTC also recommended that app stores should provide a more consistent way for developers to display information collection practices, and encouraged a layered and standardized approach, perhaps using universal icons, so that parents could better understand the nature of information collected and shared about their children.

B. Data Collection and Retention Practices

The FTC published the whitepaper "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" in 2012. It sets forth best practices for businesses to protect the privacy of consumers and give them greater control over the collection and use of their personal data. The report also recommends that Congress enact general privacy legislation, data security and breach notification legislation, and data broker legislation.

The report calls on companies handling consumer data to implement recommendations for protecting privacy, the three major components of which are privacy by design, simplified choice for businesses and consumers, and greater transparency.

The privacy by design principle states that companies should build in consumers' privacy protections at every stage in developing their products. These include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy.

The report states there should be a simplified choice for businesses and consumers. This entails companies giving consumers the option to decide what information is shared about them, and with whom. This should include a Do-Not-Track mechanism that would provide a simple, easy way for consumers to control the tracking of their online activities.

Lastly, the report encourages companies to increase their transparency. Companies should disclose details about their collection and use of consumers' information, and provide consumers access to the data collected about them.

California Attorney General's Guidelines for Mobile Application Software

The California Attorney General's Office has taken the position that "online services" under the California Online Privacy Protection Act of 2003 (Business and Professions Code Section 22575 *et seq.*, discussed above) includes mobile applications. The Attorney General and leading operators of mobile application platforms agreed to in a Joint Statement of Principles in 2012. Perhaps the most important of which is that, "where applicable law so requires, an application ("app") that collects personal data from a user must conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used and shared." Platform providers that signed the agreement include Amazon, Apple, Google, Hewlett-Packard, Microsoft and Research In Motion. The agreement was designed to help bring mobile apps in compliance with the California Online Privacy Protection Act. As a result of the app platform companies' implementation of the principles, consumers can now review an app's privacy policy in the app store, before downloading the app. An outgrowth of the agreement was to be a "best practices" paper, which industry pledged to help develop.

The California Attorney General published its privacy best practices in a 2013 whitepaper called "Privacy on the Go: Recommendations for the Mobile Ecosystem." The report addresses the issue of data privacy in the context of mobile applications. Its purpose is to serve as a template for the mobile industry to develop mobile-friendly privacy policies and practices that will improve consumer privacy. The overarching theme of the paper is a "surprise minimization" approach, which means supplementing the general privacy policy with enhanced measures to alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information.

Highlights of the recommendations: For app developers, create a data checklist to review the PII your app could collect and limit collecting data not needed for your app's basic functionality. For platform providers, make app privacy policies accessible from the app platform so they can be reviewed before a user downloads an app and increase user education on mobile privacy. For mobile ad networks, avoid using out-of-app ads and have a privacy policy. For operating system developers, in order to accommodate the smaller screens of mobile devices use special notifications such as icons, or pop-up notifications to inform consumers about how personally identifiable information is being collected and shared. For mobile carriers, leverage your ongoing relationship with mobile customers and educate them on mobile privacy.

Fair Information Practices Principles (FIPPs)

Much of the legislation created to allow individuals' access and control of information collected about them by public and private actors may be traced back to the early 1970's, and the formulation of the Code of Fair Information Practices. This is where the ideas of notice of information collection practices, individual control over information collected about oneself, and limitations on data collection and retention came from.

Fair Information Practices principles, or FIPPs have shaped and informed almost all privacy legislation in the U.S and abroad, and the same is true here in California. FIPPs are a set of internationally recognized practices for addressing the privacy of information about individuals. FIPPs are important because they provide the underlying policy for many national laws addressing privacy and data protection matters.

In a 1973 report, a U.S. government advisory committee initially proposed and named Fair Information Practices as a set of principles for protecting the privacy of personal data in recordkeeping systems in response to growing use of automated data systems containing information about individuals. The committee's charge included automated data systems containing information about individuals maintained by both public and private sector organizations. (Robert Gellman, *Fair Information Practices: A Basic History*.)

Application of FIPPs to the Mobile Environment:

As the California Attorney General recognized in *Privacy On The Go*, that document was just the latest to "encourage the alignment of architectural and functional decisions with the widely accepted Fair Information Practice Principles (FIPPs)." FIPPs, or some variation or sub-set thereof, have formed the basis for most privacy legislation – from the California Information Practices Act of 1977 (IPA), to SB 129 (Peace) Ch. 984, Stats of 2000 which created the Office of Privacy Protection and mandated all state agencies must adopt and follow FIPPs contained in the IPA, to SB 1386 (Peace) Ch. 915, Stats of 2002, which requires notification to an individual when sensitive PII about them is disclosed without authorization.

While it may be safely assumed that FIP principles may also be applied to information moving across the mobile platform, the very nature of mobile devices and the new functionality they offer, such as geo-tracking, may require separate and distinct treatment in the codes. Indeed a legal question has arisen as to whether the existing laws of California regarding informational privacy extend to information on the Internet and by extension, information moving across the mobile platform. (See discussion of *Apple Inc. v. Superior Court* (Krescent) above.) In light of this, statutory clarity may be necessary to articulate scope of the existing laws and make clear the intentions of the Legislature in this area, taking into account the unique demands of effective communication on a small and/or handheld device.

IV. SURVEILLANCE, WARRANT REQUIREMENTS, AND EMPLOYER ACCESS TO SOCIAL MEDIA

Although recent media attention has focused on the use of new technology by private advertisers to track our online behavior, these and other new technologies have also created new possibilities for physical surveillance of citizens by government, and in some cases by employers, public or private. Mobile

internet applications with tracking devices, GPS and other geo-locational devices, and Radio Frequency Identification Devices (RFID) create, for some, the Orwellian prospect that our physical movement, like our online movement, may be constantly tracked without our knowledge.[28] These new technologies have already created a body of case law – not all of it consistent – attempting to apply existing legal and constitutional principles to the use of these devices by governmental authority, especially in regard to the government's ability to access such information without a search warrant or other court order.

Fourth Amendment Principles

The Fourth Amendment of the United States Constitution provides that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath of Affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Section 13, Article I of the California Constitution mirrors the Fourth Amendment of the United States Constitution.

Under the Fourth Amendment, which protects an individual's reasonable expectation of privacy from unauthorized governmental intrusion, a search occurs when an expectation of privacy that society considers "reasonable" is infringed. The Fourth Amendment is implicated when "a person has exhibited an actual (subjective) expectation of privacy, and the expectation must be one that society is prepared to recognize as 'reasonable'." (*Katz v. United States* (1967) 389 U.S. 347, 361 (Harlan, J., concurring).)

The Fourth Amendment protects the reasonable privacy expectations of people, not places. What a person knowingly exposes to the public, even in his own home, is not a subject of Fourth Amendment protection. But what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. (*Id*. at 351.)

Generally, to inform the legitimacy of an expectation of privacy, the courts will look to precedent, public policy, and the factual circumstances of the present case. When there is no 'reasonable expectation of privacy', then government officials are not constrained by the Fourth Amendment's warrant requirement. However, if there is a 'reasonable expectation of privacy', a warrantless search of "persons, houses, papers, and effects" is "per se unreasonable" unless it falls "within some established exception to the warrant requirement." (*U.S. v. Chadwick* (1977) 433 U.S.1, 6.)

The Fourth Amendment and New Technology

The U.S. Supreme Court, along with the California Supreme Court, has analyzed a number of technological devices to determine whether their use in law enforcement constitutes a search under the Fourth Amendment.

Unmanned Aerial Vehicles and Warrant Requirements

The U.S. Supreme Court has not specifically addressed whether the use of an unmanned aerial vehicle, also referred to as a drone, constitutes a 'search'. However, aerial surveillance by an unmanned aerial vehicle combines both technological advancements in information gathering and aerial surveillance, both areas that been explored in the context of the Fourth Amendment.

When it comes to unmanned aerial vehicles there are competing privacy interests. On the one hand, a person would have no reasonable expectation of privacy in those areas within "open fields" or "curtilage" that is viewed from "public navigable space" because any member of the public could have lawfully observed from that vantage point. However, if an unmanned aerial vehicle had other technological capabilities that are not available for general public use, such as infrared sensors, to gather information from inside the home that would not have been knowable without physical intrusion, the surveillance would be a 'search' and is presumptively unreasonable. Law enforcement would then be constrained by the Fourth Amendment's warrant requirement. The question becomes what technology is in the "general public use". If the technology is within the "general public use", within the *Katz* framework, then an objectively reasonable expectation of privacy does not exist. For example, currently, there are remote control helicopters with video capabilities that are used and purchased by the general public–the same capabilities that an unmanned aerial vehicle would have, but on a smaller scale.

Electronic Tracking Devices (GPS) and Warrant Requirements

United States v. Jones, the most recent U.S. Supreme Court decision regarding the use of electronic tracking devices by law enforcement, reaffirms the principle that information gathered from a "constitutionally protected area" that would not have been knowable without a physical intrusion constitutes a 'search' under the Fourth Amendment. (See *U.S. v. Knotts* (1983) 460 U.S. 276 [a beeper placed inside a vehicle did not invade any legitimate expectation of privacy because a person traveling in an automobile on public highway has no reasonable expectation of privacy in his movements from one place to another, which were voluntarily conveyed to anyone who wanted to look]; see also *U.S. v. Karo* (1984) 468 U.S. 705 [a 'search' occurred because the agents, by using an electronic tracking device, revealed critical information about the location of an object inside the interior of the home that the government could not have otherwise obtained without a warrant.].)

In *United States v. Jones*, the Court unanimously ruled that law enforcement's warrantless attachment of a GPS tracking device to a car and subsequent warrantless use of that GPS device to track defendant Jones for a period of 28 consecutive days constituted an unreasonable search in violation of the Fourth Amendment. (*U.S. v. Jones* 565 U.S. __ [132 S.Ct. 945].) Despite the government's argument that a warrant was not needed because there is 'no reasonable expectation of privacy' on the highways, the Court held that the government's physical intrusion, by placing the GPS system in the vehicle, constituted a "search." (*Id.* at 948.)

Cellular Telephones and Warrant Requirements

In *People v. Diaz*, the California Supreme Court held that "the cell phone was immediately associated with the defendant's person and that therefore the delayed search [90 minutes following his lawful custodial arrest] of the cellular phone was a reasonable search incident to arrest." (*People v. Diaz* (2011) 51 Cal.4th 84, 93.) As incident to a lawful custodial arrest, law enforcement was not constrained by the Fourth Amendment's warrant requirements because the search was reasonable. The California Supreme Court pointed out that treating cellular phones differently because of their capacity to store information was inconsistent with *Robinson* which called for "easily applied rules" that would not be determined on a case by case basis. (*Id.* at 98.) The Court, therefore, opted for a bright-line rule that cellular phones could be searched without a warrant, as incident to a lawful custodial arrest, regardless of their storage capacity. (*Ibid*.)

Social Media/Public and Private Employer Access

Under the current statutory scheme created by AB 1844 in 2012, a private employer is prohibited from requiring or requesting an employee or prospective employee to disclose their private username or password for the purpose of accessing personal social media accounts. (Labor Code, § 980.)

V. OTHER ISSUES

Data Breach Notification and Security:

In 2003, California became the first state in the nation to require businesses and government agencies to notify affected consumers if there is a data breach that affects the consumers' personal information. According to the National Conference of State Legislatures, nearly 40 other states have subsequently adopted such laws. Under the California law, a person, business, or state agency that keeps, maintains, or leases computerized data that contains personal information must provide appropriate notices if that personal information is compromised as a result of a data breach. The law permits the person, business, or state agency to use "substitute notice" if the number of persons affected would make personal notice prohibitively expensive or impractical, or if the affected person's contact information is not available. (California Civil Code Sections 1798.29 and 1798.82.) As originally enacted, the law did not create any requirements as to the form and content of the required notices. However, SB 24 (Chapter 197, Stat. 2011) recently corrected that deficiency by requiring notices to contain specified information that will be useful to the affected resident and ensure that there is greater uniformity in the content of security breach notices. In addition, SB 24 also required that notification be sent to the state Attorney General's office for any breaches that affect more than 500 California residents. SB 24 also specified that entities covered by the Health Insurance Portability and Accountability Act (HIPAA) are deemed to have met the notice requirements of this bill if they meet the substantially similar federal notice requirements under HIPAA.

In addition to requiring businesses and state agencies to notify consumers in the event of a breach of their personal data, existing law also requires businesses to take reasonable steps to secure a customer's data. For example, when disposing of customer records, businesses are required to take reasonable steps to destroy personal information in the records by shredding, erasing, or otherwise modifying the personal information so that it cannot be read or otherwise discerned. (California Civil Code Sections 1798.80 and 1798.81.) In addition, a business that maintains personal information about a California resident must implement and maintain reasonable security procedures and practices in order to protect the information from unauthorized use, access, or disclosure. (California Civil Code Section 1798.81.5.)

Social Security Numbers

Existing law imposes various restrictions on the use of social security numbers and specifically prohibits a person or entity from doing any of the following:

- Publicly posting or displaying an individual's social security number;
- Printing an individual's social security number on any card that he or she must use to access products or services;

- Requiring an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted;
- Requiring an individual to use his or her social security number to access an Internet website unless a password is also required to access the site;
- Printing an individual's social security number on any materials mailed to him or her unless required by state or federal law. (California Civil Code Section 1798.85(a).)

Several other provisions of state law prohibit or limit the disclosure of social security numbers in specific contexts. For example, while state law requires a driver's license applicant to include his or her social security number (or other appropriate number if not a citizen) on the application, it prohibits the social security number from being included on the magnetic tape or strip used to store data on the license. (California Vehicle Code Section 12801.) Existing law also prohibits employers from displaying more than the last four digits of an employee's social security number when providing employees with an itemized statement of earnings. (California Labor Code Section 226(a).) California's Information Practices Act (discussed above) imposes certain limitations on the use, collection, and disclosure of personal information, including social security numbers, or disclosure of it in a manner that would link the information to the individual to whom it pertains without the prior consent of the individual or pursuant to a court order or some other provision of law. (Civil Code Section 1798 *et seq.*)

Both federal and state law requires the truncation of social security numbers in certain instances. For example, the federal Fair Credit Reporting Act requires a consumer reporting agency to truncate a consumer's social security number when the consumer requests a copy of his or her credit report. (15 USC 1681g.) Beginning with AB 1168 (Jones, Chapter 627, Stats. of 2007), local agencies have been implementing a social security truncation program to require the redaction of social security numbers in all public records that must be made available to the public under the California Public Records Act. (Government Code Section 27300 *et seq.*)

VI. CONCLUSION: SO WHAT ARE SOME OF THE PRINCIPAL RISKS TO PRIVACY THAT HAVE BEEN IDENTIFIED THUS FAR, AND WHAT IMPACTS ON INNOVATION WILL BE EXPERIENCED BY PLACING RESTRICTIONS ON PERSONALLY IDENTIFIABLE INFORMATION?

While recent media attention has focused to a large extent on threats posed to consumer privacy by online and mobile data collection and tracking for marketing purposes, the new technologies of the digital age have posed other threats to privacy. For example, the paper has noted that as more medical information is digitized and shared between health care providers, pharmacists, managed health care plans and other insurers – and as individuals establish and manage their own personal health records– the possibility that unauthorized persons will gain access to sensitive medical information is heightened. Although existing state and federal laws impose limits on the sharing of medical information, privacy advocates contend that they have not always kept pace with advances in online and mobile technology.[29]

The paper has also discussed how new technologies have also created new possibilities for both private and government surveillance of citizens. Mobile internet applications with tracking devices, GPS and other geo-locational devices create, for some, the Orwellian prospect that our physical movement, like our online movement, may be tracked without our knowledge.[30]

The paper has shown how these new innovative technologies have already created a body of case law – not all of it consistent – attempting to apply existing legal and constitutional principles to the use of these devices by governmental authority, especially in regard to the government's ability to access such information without a search warrant or other court order. Justice Brandeis' fear that "what is whispered in the closet shall be proclaimed from the housetops" could be paraphrased to read "what is keystroked in private shall be posted on the World Wide Web."

This paper has also explored the various advances in technology that consumers have to come to not only want, but expect from industry. In the course of accessing a favorite website or app for free there is a cost. Going online to purchase products provides consumers with speed, ease and low-costs. There is also a recognition that restrictions impact both the consumer and industry.

California is home to many of the companies that provide these products and services. They create much needed jobs to keep our state at the forefront of the new economy. The balance will be as consumers recognize the "costs" what they will be willing to sacrifice. Restrictions must be tempered with a recognition that the public may be willing to give up certain privacy protections in order to access a free website, the latest smartphone, software, app or other gadget.

Thus the paper has sought to present a broad "first look" overview for state policy-makers of many of the privacy issues and proposals that have come before the Legislature in the past several years, or are currently in the legislative hopper -- albeit with a special focus on the issue of informational privacy in the digital age. A list and brief description of the current legislative proposals appears in the Appendix of this paper.

Here, for policy-makers' consideration, is a list of just some of the kinds of important and complex policy questions these legislative proposals raise:

<u>Collection, Use, Sharing, and Tracking of PII</u>:

1. Should commercial websites and online services, including mobile application developers and platform providers, be prohibited by law from collecting and sharing a person's personally identifiable information without the affirmative opt-in consent of that person?

2. Can consumers choose to opt-out of having their data collected? Is permitting data collection usually a condition of using a website or online service? Can website operators or online services be required to offer and respect an opt-out?

3. To what extent, if at all, does existing technology permit a user of a website or online service to block the collection and/or sharing of personal information?

4. What is the current status of "Do Not Track" (DNT) mechanisms? How many browser services offer such a mechanism? Are consumers aware of these mechanisms? How user-friendly are they? If such mechanisms are widely and readily available, can websites and online services be required by law to honor a consumer's DNT request?

5. Would laws that limit or prohibit the collecting, sharing, or tracking of personal information reduce the number of free services that are available online?

6. How should the state seek to regulate, if at all, the activities of so-called "data brokers" who aggregate and resell information from a variety of sources? And is it even possible to effectively define who these entities are, let alone properly regulate their activities to ensure proper privacy protocols and consumer protections are in place in this industry?

Privacy Policies:

1. Do existing privacy policies provide consumers with adequate information and in a reasonably comprehensible fashion? To what extent should policymakers set reasonable parameters on what privacy policies should look like to ensure they are consumer-friendly?

2. Would legislation requiring that privacy policies be clearly written – perhaps even imposing length and grade-level requirements – make privacy policies more effective and useful to consumers, who must now either navigate often legalistic privacy policies containing many thousands of words, or simply hit the "accept" button and hope for the best?

3. Should privacy policies be required to be more explicit in disclosing the kinds of information that will be collected and identify the specific parties with whom information is shared?

4. Given the multiplicity of players in the Mobile App ecosystem, who should be responsible for complying with existing privacy policy requirements – for example, the app developer or the app platform? What responsibility, if any, should the consumer bear?

Medical Privacy:

1. Does the California Confidential Medical Information Act (CMIA) provide adequate protection in light of the increasing digitization of medical information and the growing popularity of personal health records?

2. How does CMIA compare to HIPAA, the federal medical privacy statute? Should CMIA and HIPAA be "harmonized," as some have advocated, or should CMIA offer more protection than the baseline protections provided by HIPAA?

3. Do our medical privacy laws need to be updated to reflect the increasing use and aggregation of genetic information?

Social Media:

1. To what extent should social media postings – such as those on Facebook or similar services – be made accessible to employers, law enforcement, or opposing litigants? Should law enforcement be required to obtain a warrant to gain access to social media content or a social media account, or does the posting of information on a social media account eliminate the poster's reasonable expectation of privacy?

2. Should parties in a legal dispute be able to access social media content as part of a discovery request? If a litigant obtains a subpoena or other court order to obtain social media content, should that subpoena or court order be directed at the user, or at the provider of the social media service?

Who Should Make The Rules?

1. Should private industry be encouraged to engage in more self-regulation by the adoption of "best practices," or should these best practices be codified in law to ensure that all businesses, not just the responsible ones, engage in best practices?

2. Should the Legislature make an effort to harmonize its own privacy statutes with the federally-proposed Consumer Privacy Bill of Rights?

3. Given the fact that the Internet does not respect political boundaries – as websites accessed in one state may be owned and operated by a business in another state or even another country – to what extent should privacy legislation come solely from the federal government and to what extent can and should the states have legitimate roles to play in setting privacy policies that work best for them?

APPENDIX A
Summary of Pending Legislation

Privacy of Personal Information Online and Mobile:

AB 242 (Chau) Privacy: Internet.
Summary: Would amend California Online Privacy Protection Act (Cal OPPA) to require the privacy policy of a commercial Web site or online service to be no more than 100 words, be written in clear and concise language, be written at no greater than an 8th grade reading level, and to include a statement indicating whether the personally identifiable information may be sold or shared with others, and if so, how and with whom the information may be shared.

AB 257 (Hall) Privacy: mobile devices.
Summary: Would amend Cal OPPA to define an online service to include mobile applications designed to be downloaded to and installed on a mobile device. The bill would require a mobile application market, as defined, to comply with specified procedures allowing access to an application's privacy policy and a means for users to report applications in violation of the applicable terms of service or law.

AB 319 (Campos) Internet Web sites and online services: minors.
Summary: Would require an operator of an Internet Web site or online service directed to minors and the operator of an Internet Web site or online service that has actual knowledge that it is collecting personal information from a minor to provide notice on the Internet Web site of what information is collected from minors by the operator and how the operator uses the information. The bill would require the operator of an Internet Web site or online service directed to minors to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from minors. This bill contains other related provisions and other existing laws.

AB 370 (Muratsuchi) Consumers: online tracking.
Summary: Current law, subject to specified exceptions, requires a business that discloses a customer's personal information to a 3rd party for direct marketing purposes to provide the customer, within 30 days after the customer's request, as specified, in writing or by e-mail the names and addresses of the recipients of that information and specified details regarding the information disclosed. This bill would declare the intent of the Legislature to enact legislation that would regulate online behavioral tracking of consumers.

AB 1291 (Lowenthal) Privacy: disclosure of a customer's personal information.
Summary: Current law requires a business to ensure the privacy of a customer's personal information, as defined, contained in records by destroying, or arranging for the destruction of, the records, as specified. Any customer injured by a business' violation of these provisions is entitled to recover damages, obtain injunctive relief, or seek other remedies. This bill would repeal and reorganize certain provisions of current law. This bill contains other related provisions and other current laws.

SB 501 (Corbett) Privacy.
Summary: Current law requires that the privacy policy identify certain information, including the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Internet Web site or online service and 3rd parties with whom the operator may share the information. This bill would declare the intent of the Legislature to enact legislation that would reform the privacy policies required for operators of Internet Web sites and smart phone applications, as specified.

SB 568 (Steinberg) Internet: minors: protection.
Summary: Would state the intent of the Legislature to enact legislation that would provide protection on the Internet for minors.

Public Agency Access to and Use of PII:

AB 179 (Bocanegra) Public transit: electronic transit fare collection systems: disclosure of personal information.
Summary: Existing law prohibits a transportation agency from selling or providing personally identifiable information of a person obtained through the person's participation in an electronic toll collection system or use of a toll facility that uses an electronic toll collection system. This bill would make these and other related provisions applicable to a transportation agency that employs an electronic transit fare collection system for payment of transit fares. The bill would require transportation agencies that obtain personally identifiable information of a person from electronic toll collection or electronic transit fare collection systems to discard that information after 6 months, as specified.

AB 487 (Linder) Vehicles: confidential home address.
Summary: Current law makes confidential the home addresses of specified governmental officers and employees and certain other persons that appear in the Department of Motor Vehicles records, if the officer, employee, or other person requests that his or her address be kept confidential, with certain exemptions for information available to specified governmental agencies. This bill would require a person who requests the confidentiality of his or her home address to provide the department with a current employment address for purposes of processing the service and collection of a traffic, parking, or toll road violation. This bill contains other related provisions and other existing laws.

AB 849 (Garcia) Protection of victims: address confidentiality.
Summary: Current law authorizes victims of domestic violence, sexual assault, or stalking to complete an application in person at a community-based victims' assistance program to be approved by the Secretary of State for the purpose of enabling state and local agencies to respond to requests for public records without disclosing a program participant's residence address contained in any public record and otherwise provide for confidentiality of identity for that person, subject to specified conditions. This bill would include victims of abuse of an elder or dependent adult, as defined, within these provisions. This bill contains other related provisions and other existing laws.

AB 1256 (Bloom) Personal information: Information Practices Act of 1977.
Summary: The Information Practices Act of 1977 provides for how an agency maintains and collects personal information. The act requires each agency to maintain in its records only personal information that is relevant and necessary to accomplish a purpose of the agency, as specified. This bill would make a technical, nonsubstantive change to these provisions.

AB 1270 (Eggman) Department of Motor Vehicles: records: confidentiality.
Summary: Current law prohibits the disclosure of the home addresses of certain public employees and officials that appear in any records of the Department of Motor Vehicles, except to a court, a law enforcement agency, an attorney in a civil or criminal action under certain circumstances, and certain other official entities. This bill would extend that prohibition, subject to those same exceptions, to the disclosure of the home addresses of code enforcement officers, as defined.

AB 1274 (Bradford) Public utilities: consumer privacy.
Summary: Would require the Public Utilities Commission, by order or rule, to require an electrical corporation or gas corporation to establish, on or before December 31, 2014, communication standards and protocols for a home area network device that communicates electrical or gas consumption data, as defined, of that device to the

electric corporation or gas corporation through an advanced metering infrastructure to ensure against the unauthorized access, destruction, use, modification, or disclosure of the data (cyber-security) and compatibility of the home area network devices.

SB 545 (Anderson) Name change Confidentiality: minors.
Summary: Would authorize a court to waive the requirements for publication and notice to a nonconsenting parent if necessary to protect the best interests of the minor upon a showing by the petitioner that the minor and petitioner are participants in a specified address confidentiality program, that the petitioner has sole custody of the minor, that the child is protected by an order pursuant to the Domestic Violence Prevention Act that prevents the nonpetitioning parent from having contact with the minor for at least 5 years, and that the nonpetitioning parent is not subject to an order to pay child support for the minor.

Medical Information

AB 658 (Calderon, Ian) Personal information: disclosure.
Summary: Would apply the prohibitions of the Confidentiality of Medical Information Act to any business that offers application software that is designed to maintain medical information to allow an individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual. By expanding an existing crime, this bill would impose a state-mandated local program. This bill contains other related provisions and other existing laws.

SB 138 (Hernandez) Confidentiality of medical information.
Summary: Would declare the intent of the Legislature to incorporate HIPAA standards into state law and to clarify standards for protecting the confidentiality of medical information in insurance transactions. The bill would define additional terms in connection with maintaining the confidentiality of this information, including an "authorization for insurance communications," which an insured individual may submit for the purpose of specifying disclosable medical information and insurance transactions, and permissible recipients. This bill contains other related provisions and other existing laws.

SB 222 (Padilla) Genetic information: privacy.
Summary: Would state the intent of the Legislature to enact legislation that would protect individuals from the unauthorized use of their genetic information, ensure that genetic information is personal information that is not collected, stored, or disclosed without the individual's authorization, provide protections for the collection, storage, and authorized use of genetic information, and promote the use of genetic information for legitimate reasons, including, but not limited to, health care, research, advancement of medicine, and educational purposes, as the field of genomics advances. This bill contains other related provisions.

SB 249 (Leno) Public health: health records: confidentiality.
Summary: Would authorize the State Department of Public Health, subject to specified provisions, to share health records involving the diagnosis, care, and treatment of HIV or AIDS related to a beneficiary enrolled in federal Ryan White Act-funded programs who may be eligible for services under the PPACA with participating entities, as defined, in health care coverage expansions under the PPACA.

SB 282 (Yee) Confidential medical information: required authorization to disclose.
Summary: Would extend provisions of the Confidentiality of Medical Information Act to require that the authorization to disclose medical information also accompany a demand for settlement or offer to compromise issued on a patient's behalf prior to the service of a complaint in any action arising out of the professional negligence of a person holding a valid license as a marriage and family therapist, as specified.

Credit Cards/Song-Beverly

SB 661 (Hill) Credit cards.
Summary: The Song-Beverly Credit Card Act of 1971 expresses the intent of the Legislature that certain provisions of the act that are similar to specified federal provisions essentially conform and be interpreted to conform to those federal provisions. This bill would make technical, nonsubstantive changes to this provision.

Data Breach Notification

AB 1149 (Campos) Identity theft: local agencies.
Summary: Current law requires any state office, officer, or executive agency that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This bill would expand this disclosure requirement to apply to a breach of computerized data that is owned or licensed by a local agency.

SB 46 (Corbett) Personal information: privacy.
Summary: Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This bill would revise certain data elements included within the definition of personal information, by adding certain information relating to an account other than a financial account.

Drones

AB 1327 (Gorell) Unmanned aircraft systems.
Summary: Would generally prohibit public agencies from using unmanned aircraft systems, or contracting for the use of unmanned aircraft systems, as defined, with certain exceptions applicable to law enforcement agencies and in certain other cases. The bill would require the acquisition of an unmanned aircraft system, or a contract for the use of an unmanned aircraft system, for authorized purposes to be subject to the specific approval of the applicable public agency's legislative body. The bill would require the legislative body, in approving the acquisition or purchase, to also adopt policies governing the use and deployment of the unmanned aircraft system. The bill would require reasonable public notice to be provided by agencies intending to deploy unmanned aircraft systems, as specified. The bill would require images, footage, or data obtained through the use of an unmanned aircraft system under these provisions to be permanently destroyed within 10 days, except to the extent required as evidence of a crime, part of an ongoing investigation of a crime, or for training purposes, or pursuant to an order of a court.

SB 15 (Padilla) Aviation: unmanned aircraft systems.
Summary: Would state the intent of the Legislature to enact legislation that would establish appropriate standards for the use of unmanned aircraft systems.

Government Use/ Warrant Issues/Penal Code

AB 249 (Donnelly) Invasion of privacy.
Summary: Existing law declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of those devices and techniques has created a serious

threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. Existing law expresses the intent of the Legislature to protect the right of privacy of the people of California. This bill would make a technical, nonsubstantive change to those provisions describing the invasion of privacy resulting from the use of those devices.

SB 467 (Leno) Privacy: electronic communications: warrant.
Summary: Current law provides for a warrant procedure for the acquisition of stored communications in the possession of a provider of electronic communication service or remote computing service. This bill would declare the intent of the Legislature to enact legislation prohibiting a government entity from obtaining the contents of a wire or electronic communication from a provider of electronic communication service or remote computing service that is stored, held, or maintained by that service without a valid search warrant.

SB 644 (Cannella) Identity theft.
Summary: Current law provides that every person who willfully obtains personal identifying information, as defined, of another person, and uses that information for an unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense. This bill would make technical, nonsubstantive changes to that provision.

Social Media/Employer Access

AB 25 (Campos) Employment: social media.
Summary: Existing law prohibits a private employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media. This bill would apply the provisions described above to public employers.

APPENDIX B
Federal Privacy Laws

General Privacy

- Administrative Procedure Act (5 U.S.C. § 500 *et seq.*). The Administrative Procedure Act establishes detailed procedures for Federal agencies to follow during administrative hearings. Provisions of the Act detail the methods by which administrators inform individuals of their rights, as well as how agencies should gather, portray and assess evidence at hearings.

- Cable Communications Policy Act of 1984 (Pub. L. No. 98-549)**.** Congress passed the Cable Communications Policy Act ("1984 Cable Act" or "Cable Act") to amend the Communications Act of 1934. The Cable Act establishes a comprehensive framework for cable regulation and sets forth strong protections for subscriber privacy by restricting the collection, maintenance and dissemination of subscriber data. The Act prohibits cable operators from using the cable system to collect "personally identifiable information" concerning any subscriber without prior consent, unless the information is necessary to render service or detect unauthorized reception. The Act also prohibits operators from disclosing personally identifiable data to third parties without consent, unless the disclosure is either necessary to render a service provided by the cable operator to the subscriber or if it is made to a government entity pursuant to a court order. The Patriot Act of 2001 narrowed the CCPA privacy provisions, clarifying that companies who offer cable-based Internet or telephone service will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only when detailed cable viewing information is being sought. Otherwise, cable operators can respond to a government surveillance request under ECPA, which does not require service providers to notify subscribers of requests.

- Census Confidentiality Statute (13 U.S.C. § 9). The Census Confidentiality Statute prohibits the use of census data for any other purpose than the original statistical purpose. The Act prohibits disclosure of census data that would enable an individual to be identified, except to officers and employees of the Census Bureau.

- Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. § 1001-1010). Congress passed the Communications Assistance for Law Enforcement Act ("CALEA", also commonly known as the Digital Telephony Act) to preserve the Government's ability, pursuant to court order or other lawful authorization, to intercept communications over digital networks. The Act requires phone companies to modify their networks to ensure government access to all wire and electronic communications as well as to call-identifying information. Privacy advocates were able to remove provisions from earlier drafts of the legislation that would have required on-line service providers to modify their equipment to ensure government access. The law also included several provisions enhancing privacy, including a section that increased the standard for government access to transactional data.

- Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 *et seq.*). This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

- E-Government Act (44 U.S.C. § 101). The E-Government Act expands e-government initiatives in the executive branch. The Act contains privacy protections, such as prohibitions on the secondary disclosure of information obtained for statistical purposes. Federal agencies are required to post machine-readable privacy policies located on their websites and to perform privacy impact assessments (PIAs) on all new collections of 10 or more persons. The Office of Management and Budget is also given authority to provide guidance to agencies on how to implement the e-government under the Privacy Act, the Government Paperwork Elimination Act, and the Federal Information Security Management Act of 2002 and to require an agency to perform a PIA on any system.

- Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2522, 2701-2711, 3121, 1367). This law amends the federal wiretap law to cover specific types of electronic communications, such as e-mail, radio-paging devices, cell phones, private communications carriers, and computer transmissions. It also extends the ban on interception to the communications of wire or electronic communication services and sets restrictions on access to stored wire and electronic communications and transaction records.

- Employee Polygraph Protection Act (29 U.S.C. Chapter 22). The Employee Polygraph Protection Act prohibits most private employers, with the exception of security service firms and pharmaceutical manufacturers, from using lie detector tests either for pre-employment screening or during the course of employment. The law does not apply to federal, local, and state governments. In the cases where polygraph testing is permitted, the testers are subject to numerous strict standards in regards to the length and conduct of the test.

- Fair and Accurate Credit Transactions Act of 2003 (Pub. L. 108–159). The Fair and Accurate Credit Transaction Act of 2003 (commonly known as FACTA) is designed to combat the growing problem of identity theft. It allows consumers to get a free credit report from each of the three major consumer credit reporting agencies (Equifax, Experian, and TransUnion) every 12 months, and to place alerts on their credit histories under certain circumstances. The law also sets standards for the masking, sharing, and disposal of sensitive financial data, such as credit card numbers and Social Security numbers. In response to FACTA, several federal agencies crafted joint regulations that require financial institutions to adopt identity theft prevention programs and take precautionary measures when dealing with identity theft "red flags," such as changes of address.

- Fair Credit Reporting Act (FCRA) (15 U.S.C. §1681-1681u). This law is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency," the credit bureaus that gather and sell information about consumers to creditors, employers, landlords and other businesses. For more information, see the FTC's Compendium of the Act at www.ftc.gov/os/statutes/fcradoc.pdf.

- Fair Debt Collection Practices Act (15 U.S.C §1692). This law was enacted to eliminate abusive debt collection practices by debt collectors, to insure that those debt collectors who refrain from using abusive debt collection practices are not competitively disadvantaged, and to promote consistent State action to protect consumers against debt collection abuses. For more information, see the FTC Fair Debt Collection guide.

- Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. §1232g). This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

- Federal Privacy Act of 1974 (5 U.S.C. §552a). This law applies to the records of federal government executive and regulatory agencies. It requires such agencies to apply basic fair information practices to records containing the personal information of most individuals.

- Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule(15 U.S.C. §§ 6801-6809). The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies. For more information, see http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

- Freedom of Information Act (5 U.S.C. § 552). The Freedom of Information Act (FOIA) provides individuals with access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information. The Act was amended in 1996 (Electronic Freedom of Information Act), so that requests for information can be made in an electronic format. FOIA procedures are not available to nonresident foreign nationals.

- Privacy Protection Act of 1980 (42 U.S.C. § 2000aa *et seq.*)**.** Congress enacted the Privacy Protection Act ("PPA") to reduce the chilling effect of law enforcement searches and seizures on publishers.
  The PPA prohibits government officials from searching or seizing any work product or documentary materials held by a "person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," unless there is probable cause to believe the publisher has committed or is committing a criminal offense to which the materials relate.
  The PPA effectively forces law enforcement to use subpoenas or voluntary cooperation to obtain evidence from those engaged in First Amendment activities. Many commentators believe the PPA extends protection to computer bulletin boards and on-line systems under the "other form of public communication" clause of the Act. However, the only case to present this question to a court, Steve Jackson Games, Inc. v. United States Secret Service, failed to resolve the issue. In *Steve Jackson Games*, the Secret Service seized a computer game publisher's electronic bulletin board system, e-mail and electronic files to search for evidence involving an employee of the company. The court decided the PPA protected the seized property, but based its decision on the fact that the company published traditional books, magazines and board games.

- Right to Financial Privacy Act (1978) (12 U.S.C. §§ 3401-3422). The Right to Financial Privacy Act was designed to protect the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. The Right to Financial Privacy Act states that "no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described" and: the customer authorizes access; there is an appropriate administrative subpoena or summons; there is a qualified search warrant; there is an appropriate judicial subpoena; or there is an appropriate written request from an authorized government authority. The statute prevents banks from requiring customers to authorize the release of financial records as a condition of doing business and states that customers have a right to access a record of all disclosures.

- Taxpayer Browsing Protection Act of 1997 (Pub. L. No. 105-35). In the mid-1990's, reports from the GAO identified thousands of cases in which IRS employees had inappropriately accessed confidential taxpayer information, and in one high-profile instance, an IRS employee had a conviction for wire and computer fraud thrown out. Congress passed the Taxpayer Browsing Protection Act to criminalize all unauthorized browsing of taxpayer information by federal or state employees and to allow civil damages for such activity.

- Telecommunications Act (1996) Customer Proprietary Network Information (CPNI) (Pub. L. No. 104-104). In the massive Telecommunications Act of 1996, Congress included a provision addressing widespread concern over telephone companies' misuse of personal records, requiring telephone companies to obtain the approval of customers before using information about users' calling patterns (or CPNI) to market new services. While the statute requires telephone companies to obtain approval before using customer's information, Congress did not specify how companies should obtain such approval. The FCC has responded in an inconsistent manner to several requests from the telecommunications industry on the type of consumer consent needed in order to release location information. The FCC issued an order interpreting the "approval" requirements in February of 1998. Under the FCC's rule, telephone companies must give customers explicit notice of their right to control the use of their CPNI and obtain express written, oral or electronic approval for its use. In August of 1999, the U.S. Court of Appeals for the Tenth Circuit abandoned the FCC privacy regulations regarding use and disclosure of CPNI.

  In U.S. West v. FCC (August 1999), the FCC responded in 2001 by ruling that opt-in consent was not required, and then changed its ruling in 2002, stating that either opt-in or opt-out consent could be used for general CPNI. The FCC also denied the Cellular Telecommunications and Internet Association's (CTIA) request for rulemaking that would have allowed opt-in consent for location information, stating that the legal language on the subject was perfectly clear. In the absence of a clear FCC ruling, the telecommunications industry resorted to self-regulatory measures. The CTIA issued a "consumer code" in September of 2003,

which asks companies to abide by their own privacy policies. States have tried to pass opt-in rulings, but the courts have struck them down.

- Video Privacy Protection Act of 1998 (18 U.S.C. §2710). The Act strictly limits the conditions under which a video rental or sales outlet may reveal information about the outlet's patrons. The Act also requires such an outlet to give patrons the opportunity to opt out of any sale of mailing lists. The Act allows consumers to sue for money damages and attorney fees if they are harmed by a violation of the Act.

- Wireless Communication and Public Safety Act (Pub. L. No. 106–81). The Wireless Communication and Public Safety Act was created primarily in response to the rise in use of mobile devices. The Act required all mobile telephones created after 2000 to have the capability to map the user's location through the use of global positioning systems. The primary benefit of such a system is that it enables 9-11 operators to locate callers in distress. However, such systems also raise major privacy concerns since they allow mobile telephone users to be located at any time. The Act clarified that telephone companies' must obtain the customer's opt-in consent to collect location information in any non-emergency situation. The Act only applies to mobile telephones, and courts have not issued any ruling about other mobile devices.

Health Information Privacy

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) - 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information. HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply. The security rule took effect on April 21, 2003. For more information, see the Web site of the federal Office of Civil Rightshttp://www.hhs.gov/ocr/hipaa/.

Identity Theft

- Federal Identity Theft Assumption and Deterrence Act of 1998 (18 U.S.C. §1028). The Act makes it a federal crime to use another's identity to commit an activity that violates Federal law or that is a felony under state or local law. Violations are investigated by federal agencies including the Secret Service, the FBI and the Postal Inspection Service and prosecuted by the U.S. Department of Justice.

Online Privacy

- Children's Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 *et seq.*). The Act's goal is to place parents in control over what information is collected from their children online. With limited exceptions, the related FTC Rule requires operators of commercial web sites and online services to provide notice and get a parent's consent before collecting personal information from children under 13. For more information, see the FTC's COPPA Web site: http://business.ftc.gov/privacy-and-security/children's-online-privacy.

- Computer Fraud and Abuse Act of 1984 (18 U.S.C. §1030). This law makes unauthorized access to "protected computers" illegal. Protected computers include U.S. government computers, computers used in interstate commerce and computers used by financial institutions. It also prohibits trafficking in computer passwords and damaging a protected computer.

- Computer Matching & Privacy Protection Act of 1988 & Amendments of 1990 (5 U.S.C. 552a (a)(8)-(13), (3)(12), (o), (p), (q), (r), & (u)). This law amends the federal Privacy Act of 1974 to set requirements that federal agencies must follow when matching information on individuals with information held by other federal, state or local agencies.

Unsolicited Commercial Communications

- CAN-SPAM Act of 2003 (15 U.S.C. §§ 7701-7713). The Controlling the Assault of Non-Solicited Pornography and Marketing Act requires unsolicited commercial e-mail messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender's physical address. It prohibits the use of deceptive subject lines and false headers in such messages. The FTC is authorized (but not required) to establish a "do-not-email" registry. The CAN-SPAM Act took effect on January 1, 2004.

- Telephone Consumer Protection Act (TCPA) (47 U.S.C. § 227). This law puts restrictions on telemarketing calls and on the use of autodialers, prerecorded messages, and fax machines to send unsolicited advertisements.

[Sources: California Office of Privacy Protection (http://www.privacy.ca.gov/privacy_laws/index.shtml); Center for Democracy and Technology (https://www.cdt.org/privacy/guide/protect/laws.php)]

ENDNOTES

[1] Apple Inc. v Superior Court of Los Angeles (Krescent) S199384 (February 04, 2013).
[2] Louis Brandeis and Samuel Warren, "The Right to Privacy," *Harvard Law Review* (1890).)
[3] *Wall Street Journal* series can be accessed at http://online.wsj.com/public/page/what-they-know-digital-privacy.html
[4] Nicholas Carr, "Tracking is an Assault on Liberty, with Real Dangers," *Wall Street Journal*, August 6, 2010.
[5] Jim Harper, "It's Modern Trade: Web Users Get as Much as They Give," *Wall Street Journal*, August 6, 2010.
[6] "Browser Makers Considering Limits on Tracking Web Users," *Sacramento Bee*, Friday, March 15, 2013.
[7] Apple Inc. v Superior Court of Los Angeles (Krescent) S199384 (February 04, 2013).
[8] "Consumer Data Privacy in a Networked World: A Framework for Protection Privacy and Promoting innovation in the Global Digital Economy", Office of the President of the United States, February 2012.
[9] Framework, pg 1.
[10] *Ibid*., pgs 11-22.
[11] *Ibid*., pg 23.
[12] *Ibid*., pg 24.
[13] Ibid., pg 29.
[14] *Ibid*., pg 31.
[15] *Ibid*.
[16] *Ibid*., pg 33.
[17] NTIA Press Release, June 15, 2012 (http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012)
[18] NTIA Press Release, February 21, 2013 (http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency)
[19] European Commission Press Release, February 6, 2013 (http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm)
[20] Wikipedia.org, "Data Protection Directive" (http://en.wikipedia.org/wiki/Data_Protection_Directive)
[21] Proskauer on International Litigation and Arbitration; Managing, Resolving, and Avoiding Cross-Border Business or Regulatory Disputes, Chapter 28 Privacy Laws, III. The European Union ("EU") Data Privacy Directive (Proskauer) (http://www.proskauerguide.com/law_topics/28/III/:pf_printable?)
[22] EU Directive, Art VI.
[23] EU Directive, Art VII.
[24] EU Directive, Art X, XI.
[25] EU Directive, Art XXVIII.
[26] EU Directive, Art. XIX.
[27] EU Directive, Art. XXV.
[28] *Ibid*.
[29] Privacy Rights Clearinghouse website: https://www.privacyrights.org/
[30] *Ibid*.