Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 825 (Levine) – As Amended March 26, 2021

SUBJECT: Personal information: data breaches: genetic information

SUMMARY: This bill would include genetic data in the definition of personal information (PI) applicable to California's Data Breach Notification Law (DBNL) as it applies to public agencies, businesses, and persons. Specifically, **this bill would**:

1) Include genetic data, as defined, in the definitions of PI in the DBNL applicable to both public agencies and private businesses and persons, if the data is acquired by an unauthorized person in combination with an individual's first name or first initial and the individual's last name.

2) Include genetic data, as defined, in the definition of PI for the purpose of the law requiring businesses that own, license, or maintain personal information to implement and maintain reasonable security procedures and practices to protect against unauthorized access, destruction, use, modification, or disclosure of that information.

3) Define "genetic data," for the purposes of California's DBNL, to mean any data regardless of its format, that results from the analysis of a biological sample from the individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source and any information extrapolated, derived, or inferred therefrom.

EXISTING LAW:

1) Provides, under the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const. art. I, Sec. 1.)

2) Requires any agency, person, or business that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the security of the system, as defined, to any California resident whose unencrypted PI, or encrypted PI along with an encryption key or security credential, was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a) and (c); 1798.82(a) and (c).)

3) Requires any agency, person, or business that maintains computerized data that includes PI that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code Secs. 1798.29(b); 1798.82(b).)

4) Requires a business that owns, licenses, or maintains PI about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PI from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code Sec. 1798.81.5.)

5) Requires, pursuant to the Information Practices Act of 1977, each agency to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the Act, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury. (Civ. Code Sec. 1798.21.)

6) Defines "PI," for purposes of the DBNL, to include either a user name or email address, in combination with a password or security question and answer that would permit access to an online account, or the individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: social security number; driver's license number or California identification card number; account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual; or information or data collected through the use or operation of an automated license plate recognition system. "PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g) and (h); 1798.82(h) and (i).)

7) Establishes the California Consumer Privacy Act of 2018 (CCPA), which gives consumers certain rights regarding their PI, as defined, such as: (1) the right to know what PI is collected and sold about them; (2) the right to request access to the specific PI the business has retained about them; (3) the right to request the deletion of the PI that the business has collected about them; (4) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age; and (5) the right to pursue a cause of action against a business that has suffered a data breach in the event the consumer's PI has been impermissibly accessed. (Civ. Code Sec. 1798.100 et seq.)

8) Requires a clinic, health facility, home health agency, or hospice to report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the Department of Health Care Services and to the affected patient or patient's representative within 15 business days of detecting the unlawful or unauthorized access, use, or disclosure. (Health & Safety Code Sec. 1280.15(b).)

9) Provides that any health care service plan that negligently discloses results of a test for a genetic characteristic to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply shall be assessed a civil penalty of at least $1,000 and not to exceed $5,000 plus court costs, unless the disclosure is pursuant to a written authorization, as specified, and, if the disclosure results in economic, bodily, or emotional harm to the subject of the test, is guilty of a misdemeanor punishable by a fine of up to $10,000. (Civ. Code Sec. 56.17.)

10) Requires, pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), that a covered entity, as defined, shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of the breach, and specifies the content and methods of notification. (45 C.F.R. Sec. 164.404.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to modernize California's Data Breach Notification Law (DBNL) to better protect the personal information of California residents and improve public accountability by adding "genetic data" to the definition of personal information (PI) which must be protected against breach through reasonable security standards and practices, and which, if acquired by an unauthorized person, necessitates notification of affected parties. This bill is author sponsored.

2) **Author's statement**: According to the author:

> Companies that make DNA home-testing kits are exempt from federal regulations safeguarding patients' medical information. Genetic information has quickly become the next frontier in consumer privacy. As of early 2019, more than 26 million consumers had added their DNA to at least one of the four leading commercial ancestry and health databases […] In recent years, there have been numerous high profile data breaches at sites like GEDmatch and Vitagene, leaving people's personal information exposed.
>
> Since there is little regulation around genetic data, these companies are left to make their own policies. California needs to step up and fill that gap just as it has previously done for data privacy. In the case of the Vitagene breach, users of the site found out that their genetic information was exposed from Bloomberg [News], not the site themselves. AB 825 updates the Data Breach Notification Law to include "genetic data" as defined in the bill in order to ensure consumers know when their data is breached.

3) **Direct-to-consumer genetic testing**: In 1990, the United States Department of Energy's Office of Science and the United States National Institutes of Health formally launched the Human Genome Project, an international scientific research collaboration aimed at mapping the human genome in its entirety. The fruits of this project were realized in 2003 when the project was declared complete. Since that time, there have been dramatic advancements in the ease and efficiency with which genetic data can be collected and analyzed.

   As genetic sequencing becomes increasingly inexpensive and accessible, it is also becoming more ubiquitous. In addition to various medical applications, the past several years have seen the rise of a growing industry for direct-to-consumer (DTC) genetic testing products. Businesses such as 23andMe and Ancestry.com market these products as opportunities to better know oneself, based on their capacity to reveal individual traits, medical predispositions, ethnicities and nations of origin, and blood relationships to others. When purchased, DTC genetic testing products provide a kit through which a sample, typically saliva, can be collected and mailed to the company for analysis. The company then provides results to the consumer, generally online, through landing pages where consumers can access

their raw genetic data as well as inferences drawn from those analyses. The information that can be extrapolated or inferred from these data continues to grow each year, as the scientific understanding of genetics and genomics improves, and new uses for databases of such genetic information continue to emerge.

4) **The unique sensitivity of genetic data**: In April of 2018, police arrested Joseph James DeAngelo, alleging that he was the "Golden State Killer" suspected of at least 13 murders, 50 rapes, and 100 burglaries in California between 1974 and 1986. Using the killer's DNA profile collected from a rape kit, investigators submitted the killer's genetic information to GEDMatch, a freely accessible genealogical database to which users upload their genetic data received from DTC genetic tests in order to identify familial matches among other users, and identified ten to twenty relatives who shared the killer's great-great-great grandparents. Investigators then reconstructed a putative family tree using this information, ultimately identifying two prime suspects, one of which was exonerated by a family member's submitted genetic data; the other, DeAngelo, was a genetic match with the killer.

   The arrest of the alleged Golden State Killer has been hailed as an exemplary use of consumer genetic data in the investigation of crimes, but it also spotlighted the issue of genetic privacy and the unforeseen uses of commercially obtained genetic data. As of 2019, over twenty-six million people had used some form of DTC genetic testing service, and that number continues to grow as new companies enter the market.[1] A 2018 publication in the leading academic journal *Science* indicated that "a genetic database needs to cover only 2% of the target population to provide a third-cousin match to nearly any person."[2]

   The capacity to reveal sensitive information about family members is not limited to the law enforcement context. A genetic test has the potential to uncover information about biological parentage and about inherited genetic traits that could reveal sensitive health conditions of parents or other relatives. Genetic data also derive particular sensitivity from the potential information that can be inferred about an individual. Already several genes associated with certain health conditions and behavioral traits have been identified, including some genotypes that have extremely high probabilities of leading to certain diseases later in life. Unlike usernames, passwords, credit card numbers, and other identifying information often subject to data breaches, genetic data cannot be changed or divorced from the individual in the event it falls into the wrong hands. This immutability extends the lifespan of compromised genetic information indefinitely, increasing the scope and duration of possible exploitation, and further amplifying its already considerable sensitivity.

   Taken together, the fact that genetic data is immutable, specific to an individual, revealing of sensitive information about kin and kinship, of ever-increasing informational value, and capable of revealing sensitive health information, renders this data unique even among categories of PI in its sensitivity. Consequently, it is critical that privacy and consumer protection laws treat these data accordingly.

---

[1] Antonio Regalado, "More than 26 Million People Have Taken an At-Home Ancestry Test," *MIT Tech. Rev.*, Feb. 11, 2019, https://technologyreview.com//s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test, accessed Jul. 23, 2020.

[2] Yaniv Erlich, et al., "Identity inference of genomic data using long-range familial searches," *Science*, 362, 690-694, (2018).

In support of this bill, the Consumer Reports and Electronic Frontier Foundation write, " We are strong proponents of public policy that bolsters consumers' privacy and their individual right to choose who accesses their data and for what purposes. It is within this framework that we support this bill, which would expand the definition of personal information in California's data breach notification and data security statutes to include genetic data. This bill would require companies to adopt reasonable security measures to protect this data from unauthorized access, and provides companies with strong incentives to comply."

5) **Data breaches at DTC genetic testing and analysis companies**: In June 2018, MyHeritage, a genealogy and DTC genetic testing service, publicly announced that it had suffered a data breach compromising the email addresses and encrypted passwords of over 92 million users.[3] The breach had allegedly occurred on October 26, 2017, eight months prior to being detected. An announcement by the company indicated that they had "no reason to believe that any other MyHeritage systems were compromised," including DNA data and credit card information, since those data were stored on separate servers.[4] In November 2019, Bloomberg News reported that Veritas Genetics, a DNA testing startup, had "recently" suffered a breach of its consumer-facing portal, but had neither issued a public statement nor acknowledged the breach on their website until it was reported in the press.[5] The company denied that there was any "theft" of data, and claimed no genetic data or health records were compromised, but offered no evidence for the claim.[6] In July 2020, GEDmatch, the same genealogy site used to identify the alleged Golden State Killer, suffered a data breach involving the use of fake profiles and unauthorized changes to users' public visibility settings that potentially compromised the data of over one million users.[7] Following resolution of the presumed vulnerability, GEDmatch noticed further attempts at unauthorized access, and ultimately shut the site down for a week to resolve any additional vulnerabilities. While representatives of GEDmatch's parent company, Verogen, publicly averred that there was no evidence any user data was compromised or downloaded during the breach, just one day later, MyHeritage announced that several users whose email addresses had ostensibly been obtained in the GEDmatch breach had received phishing emails from hackers attempting to obtain passwords to access their genetic data. At least 16 users fell victim to these phishing attacks.[8]

---

[3] Makena Kelly, "MyHeritage breach leaks millions of account details," *The Verge*, Jun. 5, 2018, https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach, [as of Mar. 25, 2021].
[4] Admin, "MyHeritage Statement About a Cybersecurity Incident," *MyHeritage Blog*, Jun 4, 2018, https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/, [as of Mar. 25, 2021].
[5] Kristen V. Brown, "Breach at DNA-Test Firm Veritas Exposed Customer Information," *Bloomberg*, Nov. 6, 2019, https://www.bloomberg.com/news/articles/2019-11-06/breach-at-dna-test-firm-veritas-exposed-customer-information, [as of Mar. 25, 2021].
[6] Zack Whittaker, "DNA testing startup Veritas Genetics confirms data breach," *TechCrunch*, Nov. 7, 2019, https://techcrunch.com/2019/11/07/veritas-genetics-data-breach/, [as of Mar. 25, 2021].
[7] Heather Murphy, "Why a Data Breach at a Genealogy Site Has Privacy Experts Worried," *The New York Times*, Aug. 1, 2020, https://www.nytimes.com/2020/08/01/technology/gedmatch-breach-privacy.html, [as of Mar. 25, 2021].
[8] Admin, "Security alert: malicious phishing attempt detected, possibly connected to GEDmatch breach," *MyHeritage Blog*, Jul. 21, 2020, https://blog.myheritage.com/2020/07/security-alert-malicious-phishing-attempt-detected-possibly-connected-to-gedmatch-breach/, [as of Mar. 25, 2021].

Although there is no evidence that genetic data was compromised in these data breaches, it is nonetheless abundantly clear that DTC genetic testing companies are prime targets for data breaches, and that malicious demand for compromised genetic data is high. As a review in the Columbia Journal of Law and Social Problems points out:

> [M]ore detailed information often proves to be more valuable in the sale to malicious actors looking to take advantage of stolen data. The informational richness and potential of genetic information is undeniable, which will likely drive its value higher than many other forms of information, as well as the incentive for theft and exploitation. […]
>
> Additionally, unauthorized use of genetic information is more difficult for the owners to detect due to a comparative lack of institutional safeguards in place to flag misuse. Individuals who have their genetic information actually used by malicious actors will lack the ability to immediately identify such occurrences. This can be starkly contrasted from situations concerning traditional data breach victims who can more easily identify misuse, such as of unauthorized credit card charges appearing on financial statements. This consideration may also increase the likelihood that malicious actors can successfully exploit stolen genetic information, further increasing the implications and risk of future harm.[9]

Recognizing the importance of protecting genetic data, the Coalition for Genetic Data Protection, a national coalition of the leading consumer genetic testing companies including 23andMe and Ancestry who would be subject to this bill's provisions, support AB 825 and write, "over the past several years, we have carefully considered the privacy and data protection issues incumbent with direct-to-consumer genetic testing services and agree that the genetic data held by our companies should be treated the same as other personal information in the unlikely event of a data breach."

Interestingly, TechNet and the California Chamber of Commerce, write in opposition that AB 825 is overbroad:

> The existing language potentially scopes a lot of other information derived from a biological sample, including health data and biometric data, into the definition of genetic data. This could create conflicts because health data and biometric data are separately defined in this code section. Creating a definition for a new term that scopes-in data that is separately defined in the law would cause confusion with regards to interpretation, enforcement, and compliance."

Staff agrees that medical information and biometric data are subject to the DBNL. Given that the requirements of the DBNL are the same regardless of what type of information is breached, overlap between the definitions of protected PI does not appear to create any confusion or additional obligations. Clearly, the sensitivity of genetic data presents a substantial risk of unauthorized access by malicious actors, and a unique risk to those whose genetic information is compromised. The difficulty in detecting the exploitation of compromised genetic data only furthers the need for the implementation of security standards and practices to protect against breach, and robust laws to ensure consumers are aware and

---

[9] Terry Wong, "Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation," *Columbia Journal of Law and Social Problems,* Vol. 53:4, pp. 500-501.

can take appropriate action if their genetic data may have been compromised. By including genetic data in the laws requiring security standards to protect against breaches and notification in the event of breaches, this bill would seemingly accomplish both of these goals.

6) **The Data Breach Notification Law (DBNL) and AB 2301**: While no general federal data breach notification laws exist, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information.[10]

SB 1936 (Peace, Ch. 915, Stats. 2002) enacted the DBNL in California, which requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data including PI, to disclose any breach of the security of the data to California residents whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Since the passage of SB 1936, the frequency and variety of data breaches has continued to increase dramatically as computing power and the public's reliance on digital information technology grow. In the United States alone, the number of reported data breaches has grown from 662 in 2010 to 1,506 in 2019, with the number of exposed records increasing 916%, from 16.2 million in 2010 to 164.68 million in 2019.[11] While these increases could result in part from increased reporting as DBNLs are adopted across the country, it is nonetheless undeniable that the quantity and sensitivity of PI transmitted and stored digitally have skyrocketed, and with them, the risk of harmful data breaches.

Accordingly, California has added numerous provisions to the DBNL in order to protect residents as data breaches become more commonplace. For example, AB 1950 (Wiggins, Ch. 877, Stats. 2004) required a business that owns or licenses PI about a California resident to implement and maintain reasonable security procedures and practices to protect PI from unauthorized access, destruction, use, modification, or disclosure. AB 1710 (Dickinson, Ch. 855, Stats. 2014) required the source of the breach to offer appropriate identity theft prevention and mitigation services to consumers at no cost, AB 2828 (Chau, Ch. 337, Stats. 2016) required notification of breaches of encrypted PI if an encryption key or security credential that could render the PI readable was also compromised in the breach, and AB 1130 (Levine, Ch. 750, Stats. 2019) added government-issued identification numbers and unique biometric data to the DBNL definition of PI.

Although genetic data is sometimes considered to fall under the definition of "biometric data," AB 1130 included in the DBNL definition of PI only "unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, *used to authenticate a specific individual*." (Civ. Code Secs. 1798.29(g)(1)(F); 1798.82(h)(1)(F); emphasis added.) It is unclear whether this was intended to include genetic data, but genetic data collected by DTC genetic testing companies or

---

[10] National Conference on State Legislatures, *Security Breach Notification Laws*, Updated Jul. 17, 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, [as of Mar. 18, 2021].

[11] Joseph Johnson, *Cyber crime: number of breaches and records exposed 2005-2020*, Statista, Mar. 3, 2021, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, [as of Mar. 18, 2021].

submitted to online databases rarely serves the purpose of authenticating a specific individual. Rather, the overwhelming majority of genetic data aggregated by businesses is for the purpose of revealing traits, characteristics, and predispositions of an individual beyond their identity, or to identify potential relatives more generally. To resolve this ambiguity and ensure that such sensitive information is subject to the same breach notification and security standards laws as other PI, in 2020, the author of this bill proposed AB 2301 (Levine, 2020), which would have added "genetic information" to the definitions of PI in the DBNL applying to persons and businesses, and to the law requiring businesses to maintain reasonable security standards and practices to protect against breaches. Due to the constraints on the legislative process imposed by the COVID-19 pandemic, however, the author elected not to move forward with AB 2301 in order to prioritize legislation addressing more pressing crises facing the State.

7) **AB 825 would ensure data breaches of genetic data would be subject to the DBNL**: AB 825 is a reintroduction of AB 2301, and, as it was introduced, was identical to its predecessor. In other words, AB 825 would have considered "genetic information," as defined, to be considered PI for the purpose of the DBNL applying to businesses and persons, and for the purpose of the law requiring businesses to implement reasonable security standards to protect against data breaches, when paired with the first name or initial and last name of an individual.

   The author has since made two significant changes to the bill in order to ensure that the vast range of genetic data that may be possessed by private and public entities is included. First, the author has amended the bill to apply to "genetic data" rather than "genetic information." This distinction is subtle, but appears to signal the author's intent to ensure a broad interpretation of the category of data included in these statutes. Generally speaking, "data" refers to any symbols representing empirical observations, whereas "information" refers to data that have been processed or contextualized to have meaning. Particularly in the case of genetic data, which can be highly technical and require significant processing to have informational value, the ability to infer meaning from the data is extremely dynamic. Raw data collected from a biological sample that may seem of little import now may ultimately yield highly sensitive information in the future as our technical capabilities and scientific understanding progress. As such, referring to "genetic data" rather than "genetic information" seems to indicate the author's recognition of the rapidly changing informational value of genetic data, and the intent to broadly define the data subject to the bill.

   Consistent with this intention, the author has defined "genetic data" expansively, to mean "any data regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material." The definition also clarifies that "genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom." In addition to accommodating the myriad ways genetic data can be determined, this definition critically includes data that is not obtained directly from a biological sample, i.e. "or from another source enabling equivalent information to be obtained." Third-party resources to analyze genetic sequence information, or to compare genetic sequence information with public databases to identify relatives, continue to proliferate. By specifying

that genetic data includes any such data that results from the analysis of a biological sample or from another source, AB 825 would ensure that the applicability of the DBNL and security standard laws extends beyond businesses that obtain genetic information from in-house analysis of a biological sample, to include other entities, like GEDmatch, that would possess similarly sensitive information.

Second, the author has included "genetic data" in the definition of PI in the DBNL applicable to public agencies in addition to the DBNL applicable to businesses and persons. Though the rise of DTC genetic testing has placed most genetic data that is not protected by medical privacy laws in the hands of private entities, genetic data is equally sensitive regardless of whether the entity possessing it is public or private. It therefore seems prudent to include genetic data in the public DBNL's definition of PI as well, both to ensure Californians can take appropriate action in the event of any data breach compromising their genetic data, and, given the significant similarity between the public and private DBNLs, to avoid complications of statutory interpretation that may result from inclusion in one but not the other.

8) **Related legislation:** AB 346 (Seyarto) would expand the DBNL for public agencies to apply to circumstances in which the PI of a California resident was, or is believed to have been, *accessed or acquired*, rather than just *acquired*, by an unauthorized person.

SB 41 (Umberg) would establish the Genetic Information Privacy Act, a comprehensive legal framework to regulate the collection, use, maintenance, and disclosure of genetic data collected or derived from a direct-to-consumer genetic testing product or service, including enhanced notice and opt-in consent requirements.

9) **Prior legislation:** AB 2301 (Levine, 2020) *See* Comment 6.

SB 980 (Umberg, 2020) was substantially similar to SB 41 (Umberg) . This bill was vetoed by the Governor.

AB 1130 (Levine, Ch. 750, Stats. 2019) *See* Comment 6.

AB 241 (Dababneh, 2017) would have required a public agency that is the source of a data breach, and is required to provide affected persons with notice of the breach, to provide at least 12 months of appropriate identity theft prevention and mitigation services at no cost to the affected persons. This bill died in the Assembly Appropriations Committee.

AB 2828 (Chau, Ch. 337, Stats. 2016) S*ee* Comment 6.

SB 570 (Jackson, Ch. 543, Stats. 2015) required, in the event of a data breach, agencies and persons conducting business in California to provide affected individuals with a notice entitled "Notice of Data Breach," in which required content is presented under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

SB 222 (Padilla, 2014) would have established the Genetic Information Privacy Act, which would have required written authorization by an individual for their DNA sample to be obtained or analyzed, as well as certain disclosures about the individual's rights to the data

and the data collection, maintenance, use, and disclosure practices of the entity handling the sample. This bill died in the Senate Appropriations Committee.

AB 1710 (Dickinson, Ch. 855, Stats. 2014) *See* Comment 6.

SB 46 (Corbett, Ch. 396, Stats. 2013) revised certain data elements included within the definition of PI under the DBNL, by adding certain information that would permit access to an online account and imposed additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves PI that would permit access to an online or email account.

SB 1267 (Padilla, 2012) was substantially similar to SB 222 (Padilla, 2014). This bill died in the Senate Appropriations Committee.

SB 559 (Padilla, Ch. 261, Stats. 2011) prohibited discrimination on the basis of genetic information, including in housing and employment contexts.

SB 24 (Simitian, Ch. 197, Stats. 2011) required any agency, person, or business that is required to issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, and required any agency, person, or business that is required to issue a security breach notification to more than 500 California residents to electronically submit a single sample copy of that security breach notification to the Attorney General.

AB 1950 (Wiggins, Ch. 877, Stats. 2004) *See* Comment 6.

SB 1936 (Peace, Ch. 915, Stats. 2002) *See* Comment 6.

REGISTERED SUPPORT / OPPOSITION:

Support

23andme
Ancestry
California Public Interest Research Group
Consumer Attorneys of California
Consumer Reports
Privacy Rights Clearinghouse

Opposition

California Chamber of Commerce (unless amended)
TechNet (unless amended)

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200