COLLISION INDUSTRY CONFERENCE

Vehicle Data Access, Privacy & Security Committee

PRESENTED BY:

CO-CHAIRS: DAN RISLEY, FRANK TERLEP

Data Privacy & Security Committee

Mission: To identify, present on and discuss topics surrounding data access, exchange and protection; and the ways in which these topics impact businesses operating within the collision repair industry.

Committee Members:

- Frank Terlep: **asTech®**
- Dan Risley: **CCCIS**
- Trent Tinsley: **ARMS Business Solutions**
- Aaron Schulenburg: **SCRS**
- Rick Palmer: **Computerlogic**
- Kelly Cooper: **1Collision**

Agenda

- Review of April Presentation (CA AB 375)
  - New Amendments
- PII
  - *What is it*
  - *How to handle PII properly*
- Privacy Work Done to Date
- Question for the Body

AB 375 Amendments Being Considered

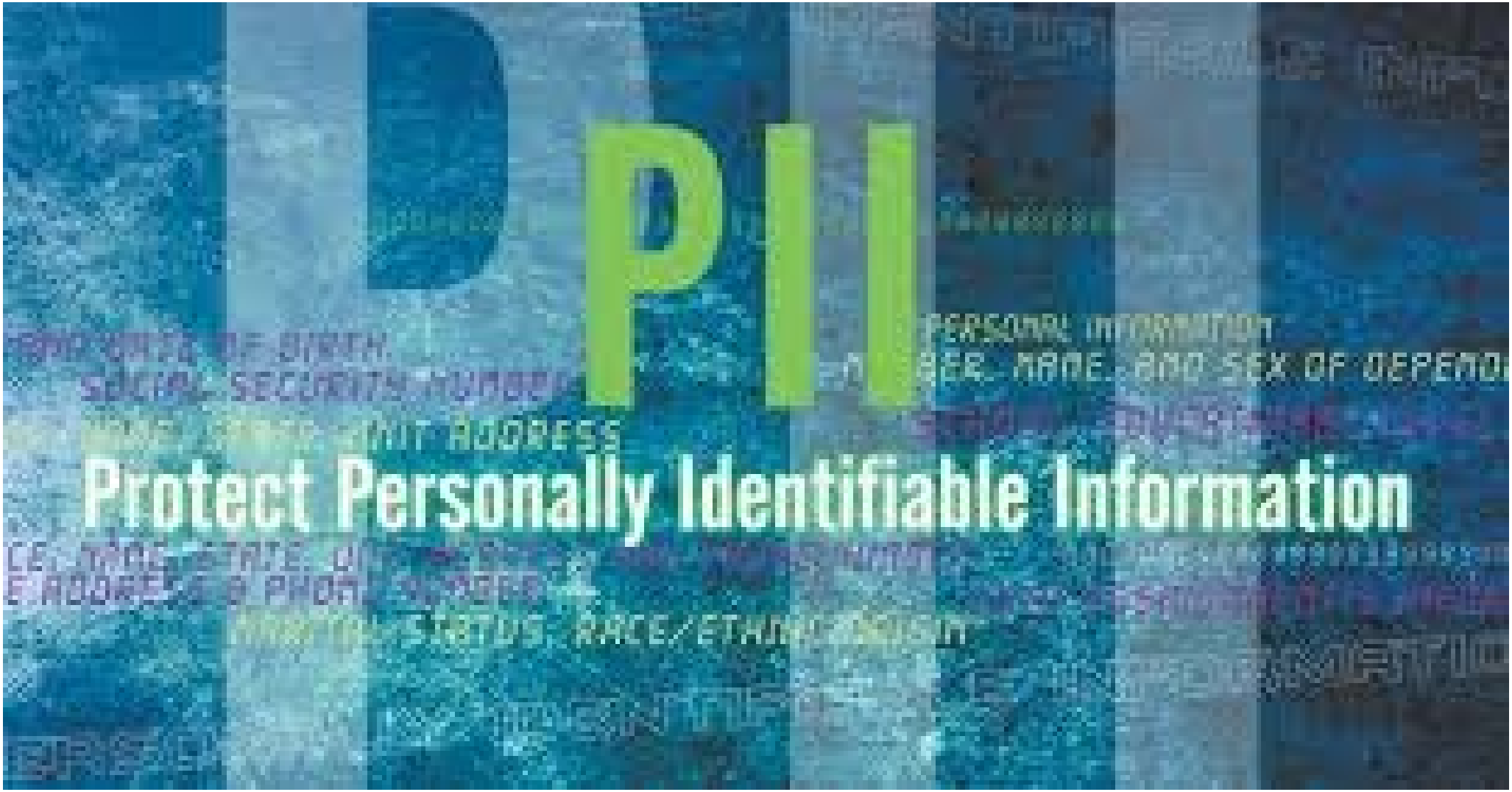
- **AB 25:** Exempts personal information if it is used for the employment
- **AB 874:** Would create a clear public record exemption from the definition of "personal information."
  - Would clarify that "personal information" does not include consumer information that is deidentified or aggregate consumer information.
- **AB981:** Would add privacy requirements to the California Insurance Information and Privacy Protection Act ("IIPPA") to reflect the CCPA and would eliminate a consumer's right to request that a business delete or not sell personal information under the CCPA if it is necessary to retain or share the personal information to complete an insurance transaction requested by the consumer.
- **AB 1146:** Would exempt certain vehicle information shared between a new motor vehicle dealer and specified parties

AB 375 Amendments Being Considered

- **AB 1355:** Would amend the CCPA to exclude consumer information that is deidentified or aggregate consumer information from the definition of "personal information."
  - Clarifies a consumer's right to request "specific pieces" of personal information must be disclosed in the business's online privacy policy or policies
  - Opt-in consent is required to sell the personal information of children less than 16 years of age (not including children who are 16 years of age).
- **AB 1416:** Would add that the CCPA shall not restrict a business's ability to comply with any rules or regulations
  - Share personal information with a government agency solely for the purposes of carrying out a government program
  - Sell the personal information of consumers who have opted out of sale for the sole purpose of detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for that activity
- **AB 1564:** Requires businesses to make available, in a reasonably accessible form to consumers, a toll-free telephone number or an email address and a physical address for submitting requests for information required to be disclosed under the law.
  - If a business maintains a website, the bill requires the business to make the website address available to consumers to submit requests for information.

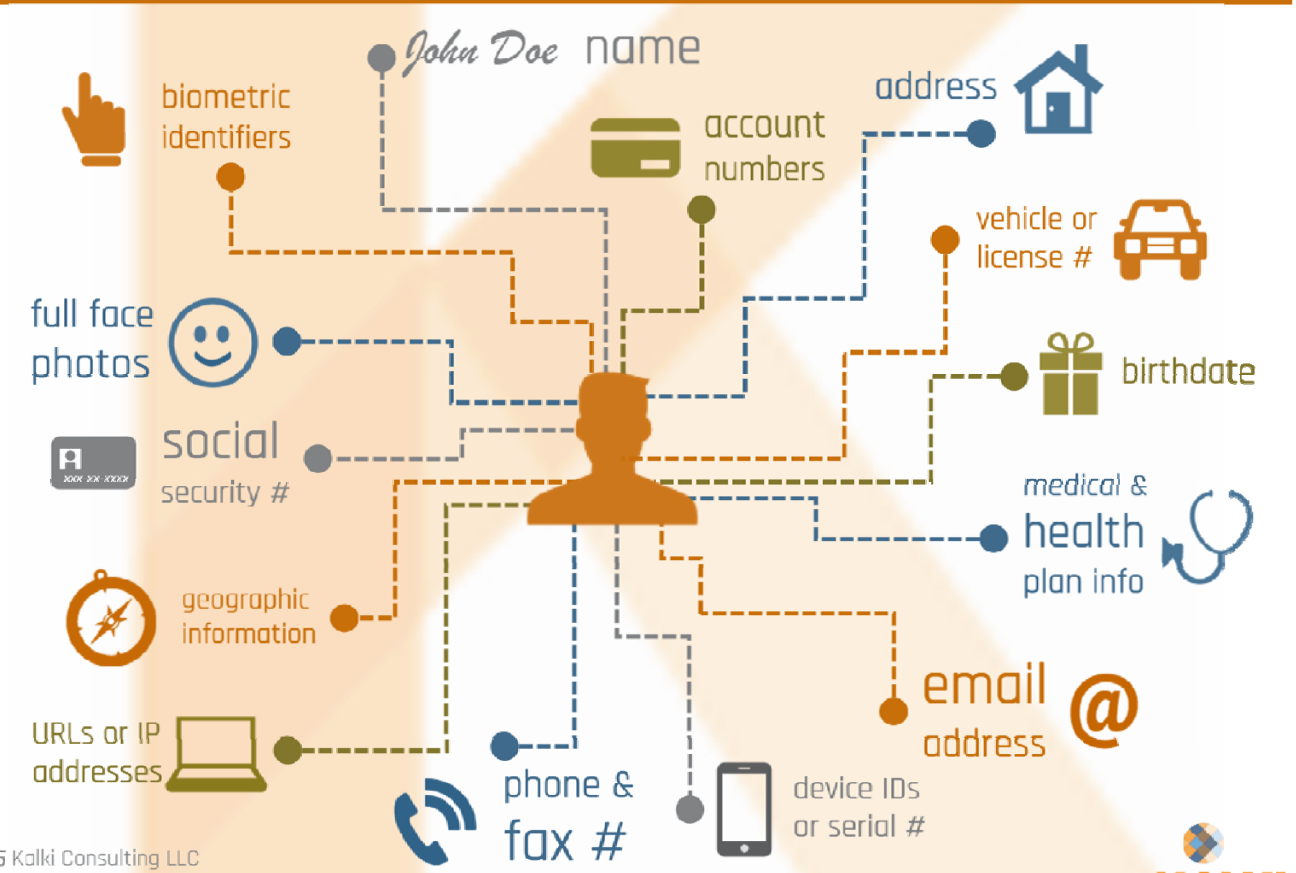
Other States Looking at Similar Laws

- **Hawaii:** SB 478
- **Maryland:** SB 0613
- **Massachusetts:** SD 341
- **Mississippi:** HB 2153
- **New Mexico:** SB 176
- **New York:** S 000224
- **North Dakota:** HB 1485
- **Rhode Island:** S 0234


PII
Protect Personally Identifiable Information

What makes up PII?

(Personally Identifiable Information)



17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554

KALKI

How to Protect PII

- **TAKE STOCK**. *KNOW WHAT PERSONAL INFORMATION YOU HAVE IN YOUR FILES AND ON YOUR COMPUTERS.*
- **SCALE DOWN.** *KEEP ONLY WHAT YOU NEED FOR YOUR BUSINESS.*
- **LOCK IT.** *PROTECT THE INFORMATION THAT YOU KEEP.*
- **PITCH IT.** *PROPERLY DISPOSE OF WHAT YOU NO LONGER NEED.*
- **PLAN AHEAD**. *CREATE A PLAN FOR RESPONDING TO SECURITY INCIDENTS.*

https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

Data & Privacy Work Occurring Within the Industry

Automotive Service Association

DATA SECURITY POLICY AGREEMENT/ADDENDUM

The purpose of this Data Security Policy Agreement/Addendum ("Agreement") is to protect and limit the unauthorized disclosure and use of "Personal Information" and "Proprietary Technical Data" (as defined herein) communicated between **[insert legal name and address of repair shop]** ("Company") and **[insert legal name and address of entity that receives data from the repair shop]** ("Vendor") as part of their business dealings. Company and Vendor shall collectively be referred to herein as "the Parties." This Agreement supplements any prior agreements between the Parties as to this subject matter and, to the extent that there is a conflict between the terms of this Agreement and any prior agreement, the terms of this Agreement shall control.

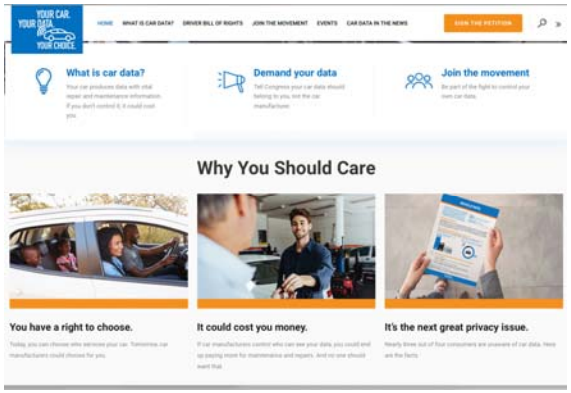
For purposes of this Agreement, the following terms have the following meanings:

(1) "Personal information" means either of the following: (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) 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; (iv) Medical information; (v) Health insurance information; (vi) Automobile insurance information; (vii) Vehicle Identification Number ("VIN"); (B) A username or email address in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) "Proprietary Technical Data" means the terms of this Agreement and any and all information, data, software, matter or thing of a secret, confidential or private nature relating to the business of the disclosing Party or its Affiliates, including matters of a technical nature (such as know-how, processes, data and techniques), matters of a business nature (such as information about costs, profits, discounts, markets, sales, customers, suppliers, the Parties' contractual dealings with each other and the projects – including preliminary, interim, or final costs, methods, scope, parts, and/or procedures used to repair one or more vehicles – that that are the subject-matter thereof), matters of a proprietary nature (such as information about patents, patent applications, copyrights, trade secrets and trademarks), other information of a similar nature, and any other information which has been derived from the foregoing information by the receiving Party; provided, however, that Proprietary Data shall not include information which: (a) is legally in possession of the receiving Party prior to receipt thereof from the other Party; (b) the receiving Party can show by suitable evidence to have been independently developed by the receiving Party or its employees, consultants, affiliates or agents; (c) enters the public domain through no fault of the receiving Party or others within its control; (d) is disclosed to the receiving Party, without restriction or breach of an obligation of confidentiality to the disclosing Party or (e) is legally required to be disclosed; provided that the receiving Party subject to such a requirement uses its reasonable best efforts to notify the other Party of any request or subpoena for the production of any Proprietary Data and provides such Party with an opportunity to resist such a request or subpoena.

autocare ASSOCIATION™

Independence drives us.



SCRS REPAIRER DRIVEN

RDN REPAIRER DRIVEN NEWS

« Back NEXT Article »

SCRS Examines Repairer Ability to Control Data Flow

By Repairer Driven News on April 24, 2014
Announcements

Share This:

Since 1994, the Collision Industry Electronic Commerce Association (CIECA) has been working with the collision repair industry to provide open standards that enable systems to communicate with each other. The use of Estimate Management Standard (EMS) has proliferated throughout the industry, and while the use of these standards have created value for participants within the collision industry framework, there have been some downsides as more and more application providers have created and installed "data sweepers" or "data pumps" that indiscriminately extract data. Many repairers are unaware of the breadth of data being extracted, where it is being extracted from, settings that would allow them to control the flow of information, or even how that information may be used beyond its intended purpose.

For years now the Society of Collision Repair Specialists (SCRS) has alerted its members about the potential risk and liability associated with inadequate control over vehicle owner data, and even data generated through participation in Direct Repair Program (DRP) agreements which may specifically include data security or privacy clauses. Until now, there have been limited mechanisms for repairers to mitigate the risk of sharing unintended information with data-sweeping programs installed on their servers, because many of these programs anonymously extract EMS files in their entirety as a background function.

COLLISION INDUSTRY
CONFERENCE

Vehicle Data Access, Privacy & Security Committee

Next Steps ?

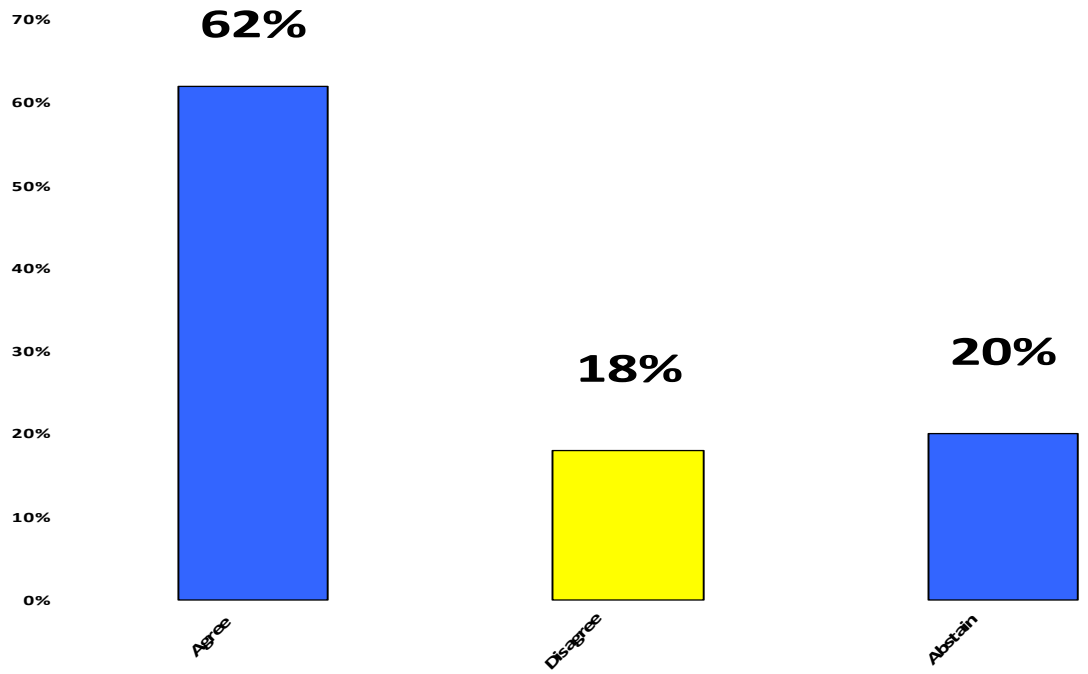
Legislative Updates

Should Legislative Committee assume responsibility for Data & Privacy Law Updates?

A. Agree

B. Disagree

C. Abstain



Should Our Committee Focus in Work Product?

Work product defined as a tutorial/guide on how to determine **WHO** is accessing your business data, **WHAT** data is being collected, HOW the data that is being collected is being used, **HOW** can I "opt out" of sharing some or all of this data?

A. Agree
B. Disagree
C. Abstain