CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice

To the NAIC Privacy Protections Working Group

April 3, 2023

In addition to our joint comments with other consumer stakeholders, CEJ submits the following comments on the draft data privacy model.

Inclusion of a Private Right of Action is Essential

It is difficult to conceive of any consumer right or protection for which a private right of action is more needed and justified than for enforcing consumer data privacy and digital rights.

First, enforcing consumer data privacy and digital rights promptly is necessary to protect consumers and deliver appropriate responses. If an insurer carelessly discloses a consumer's personal information to a stalker or criminal or is unfairly denied or priced out of critical insurance due to faulty data practices by the insurer, the physical and financial impacts for that consumer may be devastating or fatal. A consumer has a private right of action against an insurer who engages in unfair claim settlement. Surely, a consumer deserves and needs a private right of action for failure to fairly use or adequately protect personal information when the consequences of insurer failure can cause even greater damage to consumers.

Second, a private right of action is needed to assist regulators in your enforcement. Market regulators already have an immense task in enforcing a multitude of market regulations. Adding additional responsibilities for data protection involving every regulated entity creates a regulatory demand that cannot be met with existing or even modestly increased resources.

Third, much of the approach in the draft model is based on consumer protections found in the Fair Credit Reporting Act (FCRA). The FCRA includes a private right of action and that private right of action is a foundational element of the overall consumer protection scheme.

Fourth, the critical consumer protections and privacy rights in the draft model demand that insurers and other licensees face strong disincentives for lax compliance and a private right of action will provide that needed disincentive.

Definition of Adverse Action:

An adverse action based on consumer personal information can occur in parts of the insurance life cycle other than underwriting. Consequently, we suggest that adverse action be defined as:

> Any action by an insurer regarding underwriting, pricing, claims settlement, fraud detection, premium payment plans, or any loss prevention, loss mitigation, telematics or value-added services or programs offered by the licensee that results in the consumer receiving an outcome other than the most favorable outcome available to the consumer if the consumer's personal information were more favorable.

The purpose of defining adverse action is create a trigger for notice to a consumer that the licensee's use of certain information resulted in an unfavorable action for the consumer. The purpose of the notice is to alert the consumer of the adverse action and associated rights. Those rights include receiving an explanation of the adverse action, identification of the information that resulted in the adverse action, the right to verify the accuracy of the data leading to the adverse action, the right to correct any incorrect data involved in the adverse action and the right to obtain reconsideration of the adverse action using corrected data.

It should be clear that any action for which the consumer fails to receive the most favorable (available) treatment should be identified as an adverse action so the consumer is alerted and afforded the opportunity to correct incorrect information and then receive the more favorable treatment to which the consumer is entitled.

Definition of Telematics

We suggest the draft model include a definition of telematics as part of consumer-generated data. Telematics means the collection and use of personal consumer information generated by sensors in a vehicle, property or wearable device. The reason for defining telematics is to include consumer protections specific to telematics, such as prohibiting an insurer from using telematics data when it benefits the insurer, but failing to provide those data to the consumer when the data would assist the consumer.

Definition of Consumer-Generated Data

We suggest a definition of consumer-generated data for which additional consumer protections are created. Consumer-generated data include data generated by a consumer when using a mobile phone, tablet, computer or other device that captures a consumer's web browsing, social media use or tracks location, among other things.

Consumer-generated data means personal information about the consumer, vehicle or property generated by the consumer's, vehicle's or properties interaction with a sensor on or in the consumer, vehicle or property or personal information generated by the consumer's use of a mobile phone or internet-connected device including social media and internet browsing. Consumer-generated data does not include personal information provided by a consumer to a licensee as part of an application for insurance or request for benefits under a policy of insurance. Consumer-generated data does not include personal information generated solely from the licensee's administration of the insurance policy, with the exception of telematics.

Protection of Personal Information

In addition to consumer protections already set out in the draft model:

Consent by the consumer for any sharing of personal information by the licensee with any other entity not engaged in the sale or administration of the insurance. This provision applies to the licensee sharing of personal information, including consumer-generated data, with law enforcement with the following exception:

Personal information may be shared by the licensee with law enforcement without consumer consent only for purposes of investigating or prosecuting fraud in an application or claim where there is a good faith belief based on evidence available to the licensee that fraud may be occurring. Among other things, licensees are specifically prohibited from sharing consumer-generated personal information on locations visited from vehicle telematics programs or about policy services and benefits used unless there is a good faith suspicious of fraud in the use of the insurance policy.

Protection of Consumer-Generated Data

In addition to other protections for personal information, the following additional protections are required for consumer-generated data.

- Disclosure by the licensee of the licensee's intent to obtain consumer-generated data including a plain language, non-generic description of the data sought, the specific purposes for which the data will be exclusively used and the source .
-
- Consent by the consumer to the licensee obtaining the information and using the information for specifically articulated uses.

- No use for any purpose other than disclosed to the consumer.

- Delivery of consumer-generated data to the consumer upon request

- Delivery of consumer-generated data in any situation in which the data will be useful for determining edibility for benefits or services. A licensee is prohibited from failing to provide consumer-generated data to a claimant when such data will support the claimant's request for benefits.

Reliance on Massive Disclosures – the Consent Model for Data Privacy Has Failed

We note the model builds on existing privacy notices and disclosures, while largely using an opt-in approach. While having consumer opt-in as the default for insurers' collection, use and sharing of personal consumer information, we have concern about lengthy "privacy policies" and "privacy notices" that are too long to expect consumers to carefully read prior to executing a transaction and which are generally too generic and without consumer-friendly, specific use information to actually inform and empower a consumer even if they had the time to read the entire notice or disclosure.

Absent some different approach to informing and empowering consumers, additional disclosures will not producer improved data privacy. There is ample evidence and consensus among groups working on privacy that the consent model based on privacy disclosure in ineffective. For example, see the following reports:

https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right

https://www.nytimes.com/2023/02/07/technology/online-privacy-tracking-report.html

The report adds to a growing body of research suggesting that the notice-and-consent approach has become obsolete. Researchers and regulators say apps and sites often use long and sometimes unintelligible privacy policies to nudge people into agreeing to tracking practices that they may not understand. These critics say the "notice and consent" practices for online services may preclude informed consent.

Genuine "consent requires that people have knowledge about commercial data-extraction practices as well as a belief they can do something about them," the Annenberg School report said. "Americans have neither."

By this time, it should go without saying, that disclosures should be developed by experts in consumer financial disclosures and tested for effectiveness across different delivery mechanisms prior to and after deployment.

Hopefully, there is an approach to section 7 that might simplify certain disclosures while improving the content and effectiveness. Here is one suggestions:

The licensee shall disclose the data types, sources and uses of the personal information in specific, non-generic terms. Data type means a description of personal consumer information that enables the consumer to understand what characteristic of the consumer, vehicle, property, built or natural environment is being described. Sources means the direct origin of the personal information to the licensee and should be specific. Uses should be from the following list: Marketing, Determining Eligibility for Coverage, Determining Price, Determining Claim Benefits, Analyzing for Potential Fraud, Determining Payment Plan Eligibility, Preventing or Reducing Losses, Customer Relations, Other (describe). The notice could explain the uses at the top and use codes for the uses in the table.

Putting all together results in a four-column table with the fourth column reserved for the consumer's affirmative consent:

Type of Data	Source of Data	How Used	Consent?
Credit History	Experian	Marketing Determining Eligibility Determining Price Analyzing Potential Fraud	
Prior Claims History	Verisk/A-Plus	Determining Eligibility Determining Price Analyzing Potential Fraud	

FROM NAIC CONSUMER REPRESENTATIVES

To: NAIC Privacy Protection (H) Working Group

Date: April 3, 2023

Re: Recommended Revisions to Exposure Draft of Model Law #674

We the undersigned NAIC Consumer Representatives applaud the interest of the NAIC Privacy Protection Work Group in modernizing NAIC's model laws to protect the privacy of consumers' personal information. We believe the Exposure Draft of Model Law #674 is an important step toward that goal. In this communication, we recommend specific revisions to the Model Law's wording and content and identify topics for further discussion. They are shown in red. We anticipate that the NAIC Consumer Representatives will submit additional comments to the Working Group and look forward to continuing to engage with you on this important work.

ARTICLE I. Section 1. Part A (p. 3)

- **Purpose:** Revise the 4th line to *"consumers' need for fairness and protection in the collection, use and sharing of consumers' personal information."*

  We think it is important to broaden the purpose to include collection and sharing of personal information.

- **Part A (5):** Revise wording to "*Allow individual consumers to access some or all of the personal information that a licensee has collected about that consumer. ~~requesting access to verify or dispute the accuracy of the information~~; and*

  Consumers should have the right to access any of their personal information collected by the insurer and not specifically "to verify or dispute" the information's accuracy.

ARTICLE I. Section 1. Part B (p. 3)

- Scope: Revise to "*The obligations imposed by this Act shall apply to licensee and third-party services providers, who on or after the effective date of this Act:"*

ARTICLE I. Section 2 (p. 4)

- **Part A:** Delete "*or*" at the end of the second line.
- **Part B:** Revise wording of the first line to *"A licensee shall require all of the licensee's third-party service providers…"*

ARTICLE I. Section 3 (p. 5)

- **Part F (p. 6):** Although "clear and conspicuous" is a term frequently used, it is vague and likely difficult to enforce. FTC Senior Attorney Lesley Fair's commentary provides some useful information about what the term means to the Federal Trade Commission.

Her commentary suggests one way to revise the definition of "clear and conspicuous" would be:

"Clear and conspicuous notice" means a notice that is displayed prominently and for a sufficient length of time for consumers to process, is worded in a way that consumers are likely to understand, is placed (whether in print or online) where consumers are likely to look and is displayed in close proximity to other relevant information."

Another approach would be to proscriptively state "if included in a physical format, the information shall appear in a font size no smaller than 14-point type, and in a non-cursive typeface. If included on a webpage, the information shall in a font color significantly different than the other written information and shall be easily recognizable and legible."

Either approach should provide language about both the content and the presentation of the information. Our suggested language at this point currently only provides language about the presentation of the information.

In addition to our proposed clarifications for clear and conspicuous disclosures to consumers, we suggest the model law define and prohibit digital manipulation, also known as dark patterns.[1] Several states' privacy laws and federal agencies have recognized and prohibited dark patterns as a crucial component of consumers' data privacy protections.[2]

- **Part V (1) (pp. 9-10):** Delete "*or entity*" as the definition of person includes entity.
- **Part Y (1)(b) (p. 10):** Suggest that Y(1)(b) be deleted. The entire concept of affiliate is interconnectedness of decision-making. If a decision-maker at a licensee is jointly employed as a decision maker by a third party – even if there is no formal affiliation between the licensee and the company – that is an affiliated relationship.

[1] "Dark patterns are user interface techniques that benefit an online service by leading consumers into making decisions they might not otherwise make. Some dark patterns deceive consumers, while others exploit cognitive biases or shortcuts to manipulate or coerce them into choices that are not in their best interests."

"As documented in several research studies, consumers may encounter dark patterns in many online contexts, such as when making choices to consent to the disclosure of personal information or to cookies, when interacting with services and applications like games or content feeds that seek to capture and extend consumer attention and time spent, and in e-commerce, including at multiple points along a purchasing journey."
https://freedom-to-tinker.com/2022/08/10/recommendations-for-updating-the-ftcs-disclosure-guidelines-to-combat-dark-patterns/

[2] A presentation to the NAIC by the Center for Economic Justice discussed dark patterns. Slides 13 through 17 describe state and federal actions to define and prohibit dark patterns, including California, Colorado and Connecticut data privacy laws. For example, the California Consumer Privacy Act provides:
"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

"Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."
https://content.naic.org/sites/default/files/national_meeting/Consumer_Handout_CEJ_dark_patterns_SpNM.pdf

- **Part BB (1)(a) and (1)(b) (p. 11):** Replace the word "gathered" with "*collected*" to be consistent with the rest of the model.
- **Part BB (2)(f) (p. 11):** Revise to *"Information from a consumer report or an investigative consumer report."*

ARTICLE II. Section 4 (p. 16)

- **Entire Section:** Change any reference to a licensee to "*licensee or any of its affiliates*."
- **Part E (p. 18):** We applaud the requirement that licensees not be permitted to collect, process, retain or share personal information in connection with any additional permitted transactions without consumers' prior express consent. In addition, we read ARTICLE I Section 3. B. (2) (p. 5) "Research activities not related to rating or risk management purposes for or on behalf of the licensee" as excluding actuarial studies. Therefore, we have deleted actuarial studies in our revisions of the language in this section. If ARTICLE I Section 3. B. (2) was not intended to exclude actuarial studies, we look forward to conversation about the intent of that section.

  For clarity, we recommend the following rephrasing of the first and second sentences:

  "No licensee may collect, process, retain or share a consumer's personal information in connection with any additional permitted transactions without the consumer's prior express consent. Consent must be obtained for each intended additional permitted transaction. Such consent is valid for the lesser of one year or the duration of the additional permitted transaction. Once consent has been given, any person may conduct marketing or research studies and activities as follows:

  (1) For any additional permitted transactions:

  (a) No consumer may be personally identified in any study or report.

  (a) All materials allowing the consumer to be identified must be returned to the licensee that initiated the study or activity;

  (b) A consumer's personal information that may be in the data must be deleted as soon as the information is no longer needed for the specific study or activity.

  (c) The person conducting the study or activity must agree not to further share any consumer's personal information; and

  (a) A consumer's sensitive personal information may not be shared or otherwise provided to any person for use in connection with any additional permitted transaction.

- **Part F (p. 18):** Part F is overly broad. It is one thing to obtain, collect, and process de-identified information; it is a completely different thing to share that information. Sharing should be limited to the de-identified information obtained by the licensee. Sharing of that information in combination with any additional information provided by the insurer should be prohibited or limited to purposes that do not permit re-identification

of the consumer because consumers can then be identified from that information – the information is no longer reliably de-identified.

ARTICLE II. Section 5 Part B (p. 20)

- Revise the introductory sentence to this section to read: "Once the provisions of Subsection A of this section are no longer applicable to any of a consumer's personal information held by a licensee or a third party for a licensee:"
- Revise **Part B(I)**: "Such license shall completely delete and cause any third party holding personal information for the licensee to complete delete all of the consumer's personal information within 90 days after the provisions in Subsection A of this section no longer apply."

ARTICLE III, Section 7: We think this section needs much more work to ensure that consumer information practices notices provided to consumers are useful. For example, to be useful, consumers need to know the data types, sources, and uses of the personal information, described in specific, non-generic terms along with the potential risks to the consumer of licensees collecting, sharing and using this information. Research also tells us that there are more and less effective ways to communicate this information.

There are enough questions about the effectiveness of the "notice-and-consent" approach (see, for example, https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right and https://www.nytimes.com/2023/02/07/technology/online-privacy-tracking-report.html) that we need to give this section more consideration.

ARTICLE III, Section 6, C (p. 21)

- The licensee shall clearly and conspicuously identify any material changes in its information practices.

ARTICLE III. Section 7 (p. 22)

- **Parts A(1) and A(2):** These items should also require disclosure of consumer reporting agencies and data brokers that supplied consumer data that was used by licensee. To the extent that licensees or third-party service providers collect information from consumer reporting agencies and data brokers, those sources should also be disclosed. That is relevant, because the accuracy of data supplied by such sources is more likely to be suspected. A 2019 study published by the Academy of Computing Machinery found at least 40 percent of sourced user attributes sources by data brokers were not at all accurate. To make this change, revise these parts of Section 7 as follows:

A. The content of any notice required by Section 6 shall state in writing all of the following:

(1) Whether personal information has been or may be collected from any sources other than the consumer or consumers proposed for coverage, and whether such information is collected by the licensee, by a third-party service provider, by a

consumer reporting agency or by any other company that tracks and collects information about people's personal lives;

(2) *The specific types of personal information of the consumer that the licensee or any of its third-party service providers, consumer reporting agencies or any other company that tracks and collects information about people's personal lives has or may collect, process, retain, or share;*

- **Part A (12):** This section provides specific language essentially describing what clear and conspicuous means when the information is on a webpage. We suggest the addition of a parallel section describing what clear and conspicuous means in a printed notice.
- **Part B (1), C (1):** To avoid misinterpreting the language, we suggest the following revision: A statement that the consumer may, but cannot be required to, consent to the…" We also would like the model to state more clearly that without the consumer's consent the licensee cannot share the information.
- **Part C (1):** Revise end of sentence to *"… of the consumer's personal information in a jurisdiction outside of the United States and its territories."*

ARTICLE III, Section 9, B(2), B(4) (p. 27), Section 10, A(1) (28).

- The term "plain language" appears in each of these. Plain language is not defined. We suggest adding a definition or revising the language to read:
  - **Section 9, B(2):** Explain in a clear and conspicuous way that consent is being sought to use the consumer's personal information for actuarial studies by a person other than the licensee, or for research or marketing activities;
  - **Section 9, B(4):** Explain in a clear and conspicuous way that the consumer is not required to provide consent…
  - **Section 10, A(1):** Must be clear and conspicuous.

ARTICLE III. Section 10 (p. 28)

- **Entire Section:** The use of the word "authorization" in this Section is confusing. If has the same meaning as consent, then "authorization" should be replaced with "*consent*" throughout this section, because consent is used everywhere else in the Model. If authorization has a different meaning, then it should be defined in the Definitions section.
- **Part A, Part A(3), Part B, Part B(2):** As "privileged information" is defined as a component of "personal information," the words "privileged information" should be deleted.
- **Part A, Part A(3), Part A(4), Part A(5), Part B, Part B(1), Part B(2), Part B(3), Part B(4) (pp. 28-29):** As written, this section applies to the collection, processing, or sharing of a consumer's personal information. We suggest that some or all of this section should also apply to retaining information, which would require adding "retention" or "retaining" as appropriate.

ARTICLE IV. Section 12. Part A (p. 31)

- Replace "licensee" with "*licensee or third-party service provider*" or clarify that the licensee must transmit a request from a consumer to the third party within a reasonable period of time.

ARTICLE IV. Section 11. Part B(2)(b) (p.30)

- We suggest this revision: "Provide the consumer with the consumer's personal information that is in the possession of the licensee."

ARTICLE IV. Section 12. Part B(3)

- Replace "licensee" with "*licensee or third-party service provider*."

ARTICLE IV. Section 12. Part C (pp. 31-32)

- Replace "licensee" with "*licensee or third-party service provider*."

ARTICLE IV. Section 12. Part D, Part D(1), Part D(2) (p. 32)

- Replace "licensee" with "*licensee or third-party service provider*."

ARTICLE IV. Section 12, Part E(2) (p. 32)

- Revise to "*In any subsequent disclosure by the insurer, producer, or insurance support organization ....*"

ARTICLE V. Section 14 Part A (p. 34)

Section 14 of Article V protects the ability of consumers to obtain reasons for adverse underwriting decisions. We recommend three specific changes to this section:

- Revising the language to use "adverse action" rather than "adverse underwriting decisions." The reasons for this recommendation are twofold: (1) for consistency with the concept of adverse action in the Fair Credit Reporting Act, and (2) to ensure that adverse actions other than for underwriting are included. For example, if a consumer is denied approval under an accelerated life insurance program and is referred to traditional underwriting, that is an adverse action – but not necessarily an adverse underwriting decision. Similarly, if a consumer receives a premium which would have been lower if the consumer had a more favorable credit score, that is an adverse action, even if the consumer received the second best of, say, 10, premium categories.
- A requirement that the insurer provide the consumer with the reasons for the adverse action, without an option that the licensee may wait until the consumer requests the reasons. We think that allowing the licensee to require the affected consumer to submit a written request to obtain those reasons is totally unreasonable. Consumers should be given the reasons immediately, so that they can either contest the adverse decision or seek an alternative insurance transaction. Under Subsection B, it could take at least 10 business days plus the time to transmit written notification of an adverse decision and the time to transmit a request the reasons – an unnecessary and unjustifiable delay.

- Additional language to require that the reasons the licensee provides should be specific and not generic; for example, "claims history" is generic; "two claims in the past 24 months" is specific.

  Therefore, we recommend changing the wording of ARTICLE V. Section 14. Subsection A to:

  ARTICLE V. ADVERSE ACTIONS
  Section 14. Adverse Actions
  A. Notice of an adverse action. In the event of an adverse action, the licensee responsible for the decision shall provide in writing to the affected consumer at the consumer's address of record the reasons for the adverse action in specific, non-generic terms.

ARTICLE V. Section 14 Part B (2) (a) (b) (p. 34)

We would like to discuss further with you what information (and why) should be withheld from consumers if there is a reasonable suspicion of criminal or fraudulent activity and the appropriate way to address that in the model.

We also would like to discuss with you the rationale for the carve-out related to health information in this section.

ADD A NEW ARTICLE REGARDING DATA SECURITY

It has been documented that serious data breaches of personal information collected by licensees and third-party service providers occur in the insurance industry. To minimize such occurrences, it is critical that those parties adopt effective data security procedures and practices. Requirements to establish reasonable data security procedures and practices are included in the California Consumer Privacy Act and the California Privacy Rights Act, the Colorado Privacy Act, and the Virginia Consumer Data Protection Act. Model Act #674 should have such provisions too.

There are other NAIC models that include sections regarding data security. The most recent and comprehensive model is Insurance Data Security Model Law #668, which was adopted by NAIC in 2017. However, as of last fall, 30 states and territories had not adopted Model Law #668 or similar requirements in some form. Model Law #674 should either incorporate Model Law #668 provisions or establish other minimum data security requirements that licensees and third-party service providers must meet.

An example of language to address this might be: A licensee shall maintain data security protocols for personal information no less stringent than those in the NAIC Insurance Data Security Model Act. If the licensee is subject to such comparable data security standards and fulfills those standards, the licensee has met the data security requirements of this Act. If the licensee is not subject to such comparable standard, the licensee shall develop and maintain data

security protocols for personal information sufficient to meet the standards in the NAIC Insurance Data Security Model Act.

Thank you in advance for your consideration of these recommendations. If you have any questions about the content of this letter, please contact Brenda Cude (bcude@uga.edu) or Harry Ting (harry@tingnet.com).

Submitted by the following NAIC Consumer Representatives:

Brenda J. Cude

Birny Birnbaum

Erica Eversman

Kara Hinkley

Karrol Kitt

Peter Kochenburger

Harold Ting

Silvia Yee