EXPOSURE NOTIFICATION PRIVACY ACT

Section-by-Section Summary

SECTION 1. Short title; table of contents.
This Act is entitled the "Exposure Notification Privacy Act."

SECTION 2. Definitions.
[select definitions only; not an all-inclusive list]

- **Affirmative Express Consent**—an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice in response to a specific request that is provided to the individual in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms. The request must include a concise and easy-to-understand description of each act or practice for which the individual's consent is sought and must include a prominent heading that would enable a reasonable individual to identify and understand the act or practice. Affirmative express consent shall be freely given and not conditioned and shall not be inferred from an individual's inaction or an individual's continued use of a service or product.

- **Aggregate Data**—information relating to a group or category of individuals that is not linked or reasonably linkable to any individual or device that is linked or reasonably linkable to an individual. A platform operator or operator of an automated exposure notification service shall take reasonable measures to safeguard such data from reidentification; publicly commit not to attempt to reidentify such data; process such data for public health purposes only; and contractually require the same commitment for all transfers of such data.

- **Authorized Diagnosis—**means an actual, potential, or presumptive positive diagnosis of an infectious disease confirmed by a public health authority or a licensed health care provider.

- **Automated Exposure Notification Service**—any website, online service, online application, mobile application, or mobile operating system offered in commerce in the United States and that is marketed for, or specifically designed, in part or in full, to be used for, digitally notifying in an automated manner, an individual (or the device of such individual, or a person or entity that reviews such disclosures). The term does not include:

    - any technology that a public health authority uses as a means to facilitate traditional in-person, email, or telephonic contact tracing activities or similar technology that is used to assist individuals in evaluating whether they are experiencing symptoms of an infectious disease.

    - any platform operator or service provider that provides technology to facilitate an automated exposure notification service to the extent the technology acts only to facilitate such services and is not itself used as an automated exposure notification service.

- **Collect/Collection**—the buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means, including by passively or actively observing the behavior of an individual.

- **Covered Data—**any information that is linked or reasonably linkable to any individual or device linked or reasonably linkable to an individual; is not aggregated data; and is collected, processed, or transferred in connection with an automated exposure notification service.

- **Deceptive Act or Practice**—a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

- **Delete**—destroying, permanently erasing, or otherwise modifying covered data to make such covered data permanently unreadable or indecipherable and unrecoverable.

- **Executive Agency**—has the meaning given such term in section 105 of title 5, United States Code.

- **Indian Tribe**— has the meaning given such term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304) and includes a native Hawaiian organization as defined in section 6207 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7517).

- **Operator of an Automated Exposure Notification Service**—a person or entity that operates or offers an automated exposure notification service, other than a public health authority, and that is: (1) subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.), or (2) described in section 10(a)(4)..

- **Platform Operator**—any person or entity other than a service provider who provides an operating system that includes features supportive of an automated exposure notification service and facilitates the use or distribution of such service. The platform operator cannot use the technology as an automated exposure notification service.

- **Process**—any operation or set of operations performed on covered data including collection, analysis, organization, structuring, retaining, using, securing, or otherwise handling covered data.

- **Public Health Authority**—an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe that is responsible for public health matters as part of its official mandate, or a person or entity acting under a grant of authority from or contract with such public agency.

- **Service Provider**—means any person or entity, other than a platform operator, that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, a platform operator, an operator of an automated exposure notification

service, or a public health authority but only to the extent that such processing or transfer is related to the performance of such service or function.

- **State**—means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

- **Transfer**—means to disclose, release, share, disseminate, make available, allow access to, sell, license, or otherwise communicate covered data by any means to a nonaffiliated entity or person.

SECTION 3. Public Trust in Automated Exposure Notification Services

Collaboration with Public Health and Accuracy Requirements. An operator of an automated exposure notification service operator shall collaborate with a public health authority in the operation of such service. In addition, the operator may not collect, process, or transfer an actual, potential, or presumptive positive diagnosis of an infectious disease as part of the automated exposure notification service, unless such diagnosis is an authorized diagnosis. An automated exposure notification service operator also must publish guidance for the public on the functionality of the service, including any limitations related to accuracy and reliability of the exposure risk and measures of effectiveness, including adoption rates.

Prevention of Deceptive Acts or Practices. This section enables the Federal Trade Commission ("FTC" or "Commission") to seek civil penalties if a platform operator or an operator of an automated exposure notification service engages in a deceptive act or practice concerning an automated exposure notification service.

Service Provider Requirement. When a service provider has actual knowledge that an operator of an automated exposure notification service or a public health authority has engaged in an act or practice that fails to adhere to the standards in sections 3-8 of this Act, the service provider must notify the automated exposure notification service or public health authority, as applicable.

SECTION 4. Voluntary Participation and Transparency

Voluntary Participation. An operator of an automated exposure notification service is prohibited from enrolling an individual in an automated exposure notification service without the individual's prior, affirmative express consent. An operator of an automated exposure notification service must also provide an individual with a clear and conspicuous means to withdraw affirmative express consent. An individual with an authorized diagnosis shall be responsible for determining whether their diagnosis is processed as part of the automated exposure notification service.

Transparency. An operator of an automated exposure notification service and a platform operator must make publicly and persistently available—in a conspicuous and readily accessible manner—a privacy policy that provides a detailed and accurate representation of that person or

entity's covered data collection, processing, and transfer activities in connection with its automated exposure notification service.

Languages. The privacy policy required under this section must be made available to the public in all of the languages in which the person or entity provides, or facilitates the provision of, an automated exposure notification service.

SECTION 5. Data Restrictions

Collection and Processing Restrictions. An automated exposure notification service operator may not collect or process any covered data: (1) beyond the minimum amount necessary to implement an automated exposure notification service for public health purposes; or (2) for any commercial purpose.

Transfer Restrictions. An operator may not transfer any covered data, except: (1) to provide notification of a potential exposure to an individual who has enrolled in an automated exposure notification service; (2) to a public health authority for public health purposes related to infectious disease; (3) to its service provider, by contract, for certain limited purposes; or (4) to comply with the establishment, exercise, or defense of legal claims.

Further Restrictions. It shall be unlawful for any person, entity or executive agency to transfer covered data to any Executive agency unless the information is transferred in connection with an investigation or enforcement proceeding under this Act. Moreover, an Executive agency may not process or transfer covered data except for public health purposes related to an infectious disease or in connection with an investigation or enforcement proceeding under this Act.

Research Allowance. This section does not prohibit data collection, processing, or transfers to carry out research: (i) conducted pursuant to existing federal regulations regarding human subjects research; or (ii) for the development, manufacture, or distribution of a drug, biological product, or vaccine that relates to an infectious disease conducted pursuant to existing federal regulations.

SECTION 6. Data Deletion

An operator of an automated exposure notification service must delete, upon the request of an individual, the covered data of the individual. In addition, an operator shall periodically delete, on a rolling basis, the covered data of participating individuals, within 30 days or at such time consistent with a standard published by a public health authority within an applicable jurisdiction. An automated exposure notification service operator must instruct any service provider to comply with the requirements of this subsection. This section does not prohibit data retention for public health research purposes consistent with other requirements of this Act.

SECTION 7. Data Security

An operator of an automated exposure notification service shall establish, implement, and maintain data security practices to protect the confidentiality, integrity, availability, and accessibility of covered data. Such covered data security practices must be consistent with standards generally accepted by experts in the information security field.

The data security practices required under this subsection shall include, at a minimum, a risk and vulnerability assessment, corrective action to mitigate risks and vulnerabilities, and data breach notification.

This section also prohibits any person or entity from transmitting signals with the intent to cause an automated exposure notification service to produce inaccurate notifications or to otherwise interfere with the intended functioning of such a service.

SECTION 8. Freedom of Movement and Non-Discrimination

This section makes it unlawful for any person or entity to segregate, discriminate against, or otherwise make unavailable to an individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation based on covered data collected or processed through an automated exposure notification service or an individual's decision to use or not use such a service.

SECTION 9. Oversight

This section amends the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee) to allow the Privacy and Civil Liberties Oversight Board ("PCLOB") to review the government's collection, processing, and sharing of covered data in connection with a public health emergency. The section requires the PCLOB to issue a report assessing the impact on privacy and civil liberties of government activities taken to respond to the COVID-19 public health emergency no later than one year after the enactment of this Act. The PCLOB must publish a similar report no later than one year after any other Federal emergency or disaster related to a public health emergency.

SECTION 10. Enforcement

The Federal Trade Commission and State attorneys general have enforcement authority under this Act.

Federal Trade Commission: This section enables the FTC to use its existing enforcement powers and expands the FTC's jurisdiction to enforce this Act against communications common carriers and non-profit organizations. This section also empowers the FTC to seek civil penalties for first-time violations of the Act.

State Attorneys General: This section empowers the attorney general of a State, or other official or agency designated by a state, to bring a civil action in State or Federal district court to enforce this Act. Available remedies include injunctive relief, civil penalties, and other monetary relief.

Relationship to Federal and State laws: The Act preserves state laws, including state common law and state causes of action for civil relief.

Severability: If any provision of this Act is held invalid, the remainder of this Act and the application of such provision to other persons or entities not similarly situated or to other circumstances will not be affected by the invalidation.

Authorization of Appropriations and Effective Date: Funds are authorized to be appropriated to carry out this Act. The Act takes effect on the date of enactment.