Always-On Device Data Privacy Protection Act of 2017
Section-by-Section

Section 1
This section provides the short title for the bill.

Section 2
This section provides the definitions that will be used throughout the bill. Many of the definitions are newly created, based on the capabilities – current and future – of Always-on devices.

The bill explicitly covers devices such as Google Home, Amazon Echo, Apple's Siri, and Smart TVs by focusing on devices that continuously record audio, video, or image data. By including data that can be directly used to measure biometric information, the bill also looks ahead to cover devices, such as gaming systems, that generate three-dimensional images of their users using infrared light or Wi-Fi radio waves.

The bill does not cover Nest or other heat- and power grid-sensing devices, because expanding far beyond the visual and aural could inadvertently regulate the entire Internet of Things, a much larger and more complex endeavor that demands a careful look at a diverse range of devices with a variety of technological capabilities.

The bill defines Always-on device service providers broadly to include anyone offering services related to an Always-on device, including device manufacturers and entities that use information obtained from Always-on devices, including advertisers.

The bill also differentiates between Always-on device data, which is defined to mean any information obtained by an Always-on device, and a smaller set of personally identifiable information, meaning data that uniquely identifies an individual. The two categories of information are treated differently throughout the bill.

Section 3
Section 3 regulates the commercial use of Always-on devices. Based on the Video Privacy Protection Act (VPPA) and the voluntary disclosure section of the Electronic Communications Privacy Act (ECPA), the bill provides that a service provider may only disclose Always-on device data in certain enumerated circumstances, including with consumer consent, as necessary to render services, and to the government, either in an emergency or upon receipt of a probable cause warrant.

This section also lays out requirements, based on the VPPA, for obtaining consumer consent, making clear that consent must be conspicuous and separate from the "fine print" accompanying the Always-on device and that the consumer must be able to revoke his or her consent at any time. Expanding beyond the VPPA, this section requires separate consent for each type of use of Always-on device data. For example, a consumer could consent to the service provider's use of the data to improve the device but not to the use of Always-on device data for advertising.

The section requires that the consumer be informed in advance of purchasing the Always-on device if the failure to consent to a particular type of data disclosure would jeopardize the functioning of the device.

This section also makes clear that a consumer may consent only to sharing of data pertaining to his or herself. If a device is used by more than one consumer, each consumer must consent to his or her own data sharing.

Finally, this section provides that a service provider may not charge a consumer more for withholding consent for data sharing nor may a service provider offer a discount for consenting to disclosure.

Section 4

Based on CalECPA, Section 4 requires the government to obtain a probable cause warrant before obtaining Always-on device data from a service provider, from any other person or entity other than the consumer, or by means of physical interaction or electronic communication with the Always-on device in a criminal investigation.

The section provides exceptions for circumstances when the consumer has consented to the disclosure of information pertaining to his or herself and exceptions for emergencies and exigent circumstances. The emergency exceptions refer to situations when no criminal wrongdoing is suspected, a warrant could not be obtained, and the information will not be used in court, but a government entity needs to quickly obtain Always-on device data in order to save life or limb. In this scenario, the bill requires the government to file with the appropriate court a statement setting forth the grounds for the emergency so that a neutral arbiter can corroborate that there was, in fact, an emergency.

The exigent circumstances exception is based on Title III of the Wiretap Act and allows the Attorney General or principal prosecuting attorney in any state to authorize the acquisition of Always-on device data in a law enforcement emergency where there is immediate danger of death or serious bodily injury or a threat to national security and there are grounds upon which a warrant could issue. In this scenario, the bill requires the government to obtain a warrant within 48 hours after Always-on device data acquisition begins. This section is enforceable by a suppression remedy.

Section 5

This section requires actual notice to the Always-on device consumer when the government has obtained his or her Always-on device data. In the context of e-mail and other records held by third parties, the government has contended that it satisfied the notice requirement attendant to Rule 41 by notifying the service provider. This section ensures that the government notifies the individual whose data has been collected.

Mirroring language in ECPA, this section also provides for delayed notification if immediate notice would endanger the life or safety of an individual, seriously jeopardize an investigation or unduly delay a trial, or engender flight from prosecution, destruction of or tampering with evidence, or intimidation of potential witnesses. This section deliberately adopts longstanding

language from existing law that courts and law enforcement agencies are accustomed to interpreting.

Section 6

This section requires service providers to maintain a consumer dashboard or other interface that permits consumers to view and permanently delete Always-on device data pertaining to themselves. Based on the VPPA, it also requires service providers to proactively delete consumers' Always-on device data no later than two years after the information is no longer necessary for the purpose for which it was collected unless the consumer has requested that the data be saved. The two-year limit on data retention should provide service providers with ample time to use the collected Always-on device data to improve their products and to innovate.

The section also allows the government to issue a preservation request, requiring that information be preserved pending the issuance of a warrant, and requires the retention of data that is subject to a warrant or preservation request, notwithstanding a consumer's request for deletion. The concept of a preservation request is based on state-level laws governing automatic license plate readers in Utah and Vermont.

Section 6 also endeavors to protect the privacy of third parties, who cannot practically consent to the recording, transmission, and retention of their personally identifiable information. In many cases, they may not even be aware that they have come in contact with an Always-on device. Therefore, this section requires service providers, to the extent possible, to program their Always-on devices to distinguish between the personally identifiable information of the consumer and the personally identifiable information of individuals other than the consumer. The legislation then requires service providers to permanently delete personally identifiable information pertaining to individuals other than the consumer. The deletion requirement specifically applies to a smaller subset of information – personally identifiable information – out of recognition that service providers may have a legitimate interest in maintaining some Always-on device data to aid in product improvement. This compromise aims to balance third parties' privacy interests – by deleting the most sensitive information collected – with service providers' interests in innovation. This section provides exceptions for devices, such as those meant to aid the visually impaired or the hard of hearing or those that monitor infants, the elderly, or the disabled, that require the retention of personally identifiable information about third parties in order to perform their intended function.

Section 7

Section 7 provides for data security. It does this first, based on Illinois' Biometric Information Privacy Act, by requiring service providers to adhere to industry standards for the secure storage, transmission, and protection of Always-on device data.

However, borrowing an idea from Washington State's law on facial recognition matching systems for driver's licenses, the bill also allows an executive agency to promulgate security standards for Always-on device data storage, transmission, and protection. The bill, which allows the Federal Trade Commission (FTC) to set such standards, provides that these standards will only preempt industry practices if they are more protective than industry standards. This dual layer helps protect against a "race to the bottom" in industry standard setting, but also

provides for a standard should the FTC fail to act or should the FTC promulgate insufficiently protective standards.

Section 8
This section provides for a private right of action against a service provider that improperly discloses or stores Always-on device data or personally identifiable information in violation of the statute.

Section 9
This section provides that the bill is enforceable by the FTC as a violation of the Federal Trade Commission Act rule on unfair or deceptive acts or practices. It also allows for enforcement by state attorneys general.

Section 10
Section 10 provides that this bill preempts only the provisions of state or local law that require disclosure that is otherwise prohibited by the bill.