SECTION-BY-SECTION SUMMARY

Section 1. Short Title

This section provides the short title of the bill as the Suspicion-Enhancing Tools of Predictive Policing Systems Act or the STOPPS Act.

Section 2. Definitions

This section defines predictive policing systems to include any computer-based tool used by law enforcement to make inferences about crime, but it excludes computer-based tools used solely for basic tasks such as storing, searching, communicating, and retrieving police records. For example, a computer in a patrol car running software to retrieve a person's criminal history or to search a stolen vehicle database is a "basic computer-based policing system." Alternatively, software for generating and viewing crime heatmaps, risk assessment scores, or automatically searching facial recognition databases for potential suspects is considered by this Act to be a "predictive policing system." If a single computer executes both types of software, then the use of the computer as part of a predictive policing system would be affected by this Act, but the use of the computer as part of a basic computer-based policing system would not.

This section additionally defines the scope of our legislation to stops based on reasonable suspicion with a number of exceptions.

Section 3. Use of Predictive Policing Systems for Reasonable Suspicion

This section sets forth rules to strengthen the reasonable suspicion standard for investigatory stops in which PPS is used by an officer, as stated in subsection (a).

First, subsection (b) describes permitted uses of information generated by PPS during stops for the purpose of establishing reasonable suspicion. Paragraph (b)(1) outlines the primary use limitation. It requires information generated by PPS to be reasonably related to the suspected crime, directly connected to the suspected individual, and derive from PPS in compliance with subsection (g) of section 4. The subsection incorporates "reasonable relation" language from *Terry v. Ohio*, 392 U.S. 1 (1968), a case in which the Supreme Court held that to justify the reasonableness of a stop, "the police officer must be able to point to specific and articulable facts" that support a reasonable suspicion "that criminal activity may be afoot." The Act clarifies this standard in the context of PPS where the Court has never expressly ruled; the information must reasonably relate to a specific offense or criminal activity. Additionally requiring the aggregated information to directly connect to the suspected individual accounts for circumstances in which inferences might be made based on the individual's relationships.

Second, subparagraph (b)(2)(A) establishes that information generated by PPS that fails to meet the dual requirements outlined above may still contribute to an officer's evaluation of the

totality of the circumstances towards providing reasonable suspicion to make a stop. This subparagraph generalizes and codifies the holding in *Illinois v. Wardlow,* 528 U.S. 119 (2000) ("An individual's presence in a 'high crime area,' standing alone, is not enough to support a reasonable, particularized suspicion of criminal activity, but a location's characteristics are relevant in determining whether the circumstances are sufficiently suspicious to warrant further investigation."), expanding the totality of the circumstances doctrine from presence in a high crime area to any information generated by PPS that does not satisfy paragraph (b)(1).

Third, subparagraph (b)(2)(B) enumerates certain types of PPS-based information that cannot establish reasonable suspicion alone. Though limited to information generated by PPS, the provision reinforces that factors such as hotspots (similar to high crime area prohibited by *Illinois v. Wardlow*), criminal history (prohibited by numerous state courts), identity (to preclude stops based solely on target lists), and social-network associations (such as gang membership) can only, as a matter of policy, be one factor in the totality of circumstances determination that reasonable suspicion requires. In other words, an officer would need more than one of these types of PPS-based information to establish reasonable suspicion. And even then, the PPS-based information can only contribute to the the totality of the circumstances towards providing reasonable suspicion, unless the PPS-based information taken together satisfies paragraph (b)(1).

Fourth, paragraph (b)(3) accounts for the circumstance in which a crime has recently been committed in the surrounding area and is therefore still considered to be imminent or ongoing rather than a past crime. The "reasonable inference" and "virtual certainty" language comes from *People v. Flores*, 12 Cal. 3d 85 (1974), a case addressing stops of individuals present near recent crime areas. The permissible factors for an officer to consider—apart from a particularized description of the perpetrator or vehicle—have been adapted to account for information that can now be predicted by PPS, such as the size of the recent crime area, the number of individuals present in the area, and the direction or trajectory of the perpetrator.

Fifth, paragraph (b)(4) requires officers to make a good faith effort to consider known or readily-available exculpatory information from PPS or basic computer-based policing systems used when determining whether to make a stop. As the amount of information readily available to officers increases, there is a danger that selectively focusing on inculpatory information may erode the protection of the reasonable suspicion standard. This provision is intended to mitigate this erosion.

The final use limitation in paragraph (b)(5) proactively provides basic protection for individuals predicted by PPS to commit *future* crime. Officers must obtain consent to stop them.

Subsection (c) grants judges the discretion to deny or reverse findings of reasonable suspicion under subsection, while subsection (e) excuses noncompliance with paragraphs (b)(1), (b)(2), and (b)(4) in the event of emergencies and allows for stops to be made based solely on identity if an individual is wanted for a completed felony in accordance with *U.S. v. Hensley*, 469 U.S. 221 (1985).

Section 4. Accountability and Oversight

This section provides six measures to ensure the accountability and oversight of state and local law enforcement agencies. First, it requires officers to log the use of PPS if it is being used to establish reasonable suspicion and transmit the log to the law enforcement agency. The log includes predictive policing systems used, data outputs considered, potentially exculpatory information considered, and whether the stop resulted in an arrest.

Second, it directs each law enforcement agency to allow individuals filing a complaint and criminal defendants to access relevant logs. Each law enforcement agency must develop measures to prevent unauthorized access or release of the log and comply with the State's public disclosure laws. This requirement is based on criteria in The Leadership Conference on Civil and Human Rights & Upturn, *Police Body Worn Cameras: A Policy Scorecard* app. 1, criterion 4 (2015).

Third, this section establishes the Office of the National Coordinator of Predictive Policing ("the Office") within the Department of Justice and the Predictive Policing Policy and Standards Committee ("the Committee"). The Office is headed by the National Coordinator, charged with establishing and directing the operations of the Committee, maintaining and updating an Internet website that details the Committee's work and recommendations, endorsing standards recommended by the Committee, adopting a model use policy, establishing a process for the certification by law enforcement agencies, and preparing various annual reports.

The Committee makes policy and standards recommendations relating to the appropriate use of PPS to the National Coordinator by proposing a use policy framework that includes standards for the appropriate use of PPS and PPS data management procedures. The Committee allows public input through open meetings. The Committee membership includes fifteen members representing a broad range of actors that serve on three-year staggered terms. Additionally, the Attorney General provides for publication in the Federal Register. The structure and duties of the Office and Committee are based on sections 3001 through 3004 of the American Recovery and Reinvestment Act of 2009, which created the Office of the National Coordinator for Health Information Technology to coordinate national efforts to implement and use the health information technologies and the electronic exchange of health information.

Fourth, this section requires each state and local law enforcement agency that uses PPS and receives federal funds for such use to adopt and enforce a use policy that incorporates each standard set out in the model use policy. The adoption and compliance with section 3 must be certified on an annual basis. Further, each law enforcement agency must develop an annual strategic plan and conduct open meetings and allow for public comment before adopting the model use policy or when making substantial changes. This section is based on Minnesota (HF 543/SF 466) and Illinois (HB 221) bills, which provide model policies for the investigation of

officer-involved deaths and police body cameras.

Fifth, this section directs each law enforcement agency to develop ongoing, comprehensive training programs for all personnel who may use or be involved with the use of PPS. This requirement is based on Andrew Guthrie Ferguson's suggestion in *Policing Predictive Policing*, 94 Wash. U. L. Rev 1, 57 (2017).

Sixth, this section requires an internal and external audit of the use of PPS. The internal audit must be conducted annually to evaluate compliance with the adopted use policy and the strategic plan by any law enforcement agency using PPS, and the results of the internal audit must be considered to improve the use policy and PPS-related training programs.

The external audit must be done by the Criminal Justice Information Services Division of the FBI (the "CJIS"). The CJIS will audit each PPS in use by a law enforcement agency, including the system's use, frequency of use, success rate of the system, and potential for disparate impact. Additionally, the CJIS will audit the data used by PPS by examining collection, maintenance, accuracy, access, and verification procedures. Further, CJIS must be granted access to the systems, data, documentation, and policies, along with the cooperation of the law enforcement agency and the developers of the PPS under audit. The completed audits must be reported annually to the Attorney General, who may request additional information or testimony and must subsequently release the report. The requirements, duties, and structure are partly derived from a Wisconsin law (AB 409) that sets standards for investigations in local law enforcement agencies of officer-involved deaths while wearing police body cameras.

Finally, this section directs the Attorney General to make funds available to States and units of local government, or combinations thereof, for programs or projects that fall under section 4. The funds come from the Edward Byrne Memorial Justice Assistance Grant Program, under which funds are currently provided for the Smart Policing Initiative.

Section 5. Enforcement

The first enforcement mechanism requires the suppression of any results or evidence that is derived therefrom if an officer violates the requirements of section 3.

The second mechanism establishes a private right of action for any person who is stopped based on the use of PPS in violation of the requirements under section 3. That person may recover from the officer who did not comply with section 3 or from the law enforcement agency that employs such officer. There are three available exclusive reliefs: first, equitable or declaratory relief, such as orders requiring the officer to stop violating the requirements under section 3; second, damages suffered by the claimant, which may include emotional distress and actual economic loss; and third, reasonable attorney's fees and other litigation costs reasonably incurred, which may include court fees and other related fees, hiring expert witnesses, and the costs of a study. As a complete defense, the officer or the law enforcement agency must show

that the officer made a good faith determination that an exception under subsection (e) of section 3 applied. Finally, there is a two-year statute of limitation that does not have to start on the same date as the stop. The language on the private right of action is based on the Electronic Communications Privacy Act, section 2520 of Title 18 of the U.S. Code.

Section 6. Funding for Law Enforcement Predictive Policing Systems

This section conditions federal financial assistance and funds for the creation, maintenance, or modification of law enforcement predictive policing systems on the annual certification of compliance with sections 3 and 4. Further, this section takes effect 18 months after this Act's enactment.