Congress intended to protect existing privacy rights through the passage of the Driver's Privacy Protection Act of 1994 (DPPA).

- Illegal to obtain, use or disclose driver's license information unless it is for one of the limited purposes permitted by the DPPA.
- Criminal penalties and civil remedies.
  "...[T]his is a fundamental issue of privacy. The Supreme Court has found that people have a right to be safe in their homes, that they have a right not to have the Government make public their personal data and that Congress can use its powers-section 5 of the 14th amendment-to provide remedies for violations to constitutional rights." 139 Cong. Rec. S15745-01 S15763 (1993) (Sen. Boxer).
- *Maracich v. Spears*, 133 S. Ct. 2191 (2013) - the Supreme Court of the United States found that the DPPA protects the "most sensitive kind of information," and the use of "this highly personal information" was a "substantial intrusion on privacy." (*Id.* at 2194).

The Statute Continues to be Widely Abused

- In 2012 in Minnesota, the State Office of Legislative Auditor found that 50% of officers were misusing the DVS database.
- Captain John Hunt, the DNR Compliance Officer charged with training DNR employees on the DVS database, was terminated after he obtained over 5,000 individuals DL information over 19,000 times, 94% of them were women. Ironically, Hunt was in charge of training others in the proper use of this database.
- Police officers have obtained and continue to obtain the private information of well-known individuals in the community, such as news reporters, along with the private data of fellow officers and their family and friends, including:
  - Jessica Miles (Kampschroer)[KSTP] – over 1350 accesses
  - Alix Kendall (Fox 9) – over 3700 accesses
  - Dawn Mitchell (Fox 9)– over 200 accesses
  - Beth McDonough (KSTP)- nearly 500 accesses
- Officers are looking at social security numbers, medial information given to the DMV, home addresses, weights, ages, and all driver's license photos ever taken.