UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Kirsten Hagen Kennedy Plaintiff, v. City of Braham; Robert Knowles, in his individual capacity as the Chief of Police for the City of Braham; Michael Campion, in his individual capacity as the Commissioner of the Department of Public Safety; Ramona Dohman, in her individual capacity as the Commissioner of the Department of Public Safety; John and Jane Does (1 - 100) acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other governmental agencies; Department of Public Safety Does (1-30) acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; and Entity Does (1-30) including cities, counties, municipalities, and other entities sited in Minnesota, Defendants.	Civil File No. **COMPLAINT** **JURY TRIAL DEMANDED**

For her Complaint, for which she demands trial by jury on all claims so triable, Plaintiff Kirsten Kennedy ("Kennedy") hereby states and alleges as follows:

INTRODUCTION

This is a case to redress the abuse of power by numerous law-enforcement personnel and public employees who impermissibly accessed the Minnesota Department

of Public Safety's system for maintaining the personal, private information of Minnesota citizens. Officers and employees from approximately several different law-enforcement agencies and entities chose to violate federal law, Minnesota and federal policy and the constitutionally and statutorily protected privacy rights of Plaintiff Kirsten Kennedy ("Kennedy").

These personnel violated the federal Driver's Privacy Protection Act ("DPPA") and violated Kennedy's civil rights under 42 U.S.C. § 1983, by unlawfully accessing her protected driver's license information without any legitimate purpose. More disturbing, these personnel, charged with protecting and serving the public, knowingly abused her position of trust simply to satisfy their shallow desires to peek behind the curtain into the private life of Kennedy, without her knowledge or consent, and without ever informing her of their activities. The utter disregard for her privacy rights by law-enforcement personnel, public employees, and others caused Kennedy emotional distress and a logical fear for her personal safety.

In particular, City of Braham Police Chief Robert Knowles, a leader in Kennedy's church, obtained this information 48 times without her knowledge. When confronted, Chief Knowles sought to cover up his behavior and coerce Kennedy into falsely saying she consented to it and into giving up her claims, admitting by his conduct that he had violated the law.

The State of Minnesota, itself, has found that at least 50% of all officers statewide are engaged in the use of this database for impermissible purposes, and therefore violating federal civil and criminal laws. Moreover, the access permitted to law-

enforcement officers, public employees, and others is easily obtained and makes highly private information available, including health information and social security numbers. Kennedy has no control over the Defendants accessing of her personal information, and impermissible, and inappropriate accessing has been deliberately concealed and conducted in a surreptitious fashion. These Defendants are the window-peepers of the electronic data age. Through lax policies and apathetic enforcement of the law, these officials and governmental units have caused direct damage to Kennedy, just as they have trampled upon the clear legislative protections of all citizens' right to feel secure in their privacy.

General Background of Law and Facts

1. This is an action for injunctive relief and money damages for injuries sustained when personnel from various entities in Minnesota illegally obtained Kennedy's private, personal and confidential driver's license information without a legitimate or permissible law-enforcement purpose or any other lawful purpose.

2. These law-enforcement personnel, public employees, and others viewed and obtained Kennedy's private information approximately seventy-one times between 2007 and 2013.

3. Attached to this Complaint as Exhibit A is a copy of an audit prepared by the Minnesota Department of Public Safety showing the accesses of Kennedy's driver's license information by name, not license plate number, with her driver's license number removed, and showing the "station," meaning the police department, sheriff's office, or other government entity through which the officer accessed her information.

4. Without legitimate, permissible reasons, these individuals obtained Kennedy's private information from Department of Vehicle Services' ("DVS") database or Bureau of Criminal Apprehension ("BCA") database.

5. Upon information and belief, these individuals further impermissibly used or disclosed Kennedy's private information.

6. Each unauthorized, impermissible use, disclosure, or access of her private information, made while acting under color of state and federal law, violated Kennedy's federal civil rights and constituted behavior prohibited by the federal constitution, federal statute, Minnesota statute, common law, and agency and departmental regulations prohibiting some or all of the conduct engaged in by Defendants in this case.

7. Kennedy brings this action pursuant to 42 U.S.C. §§ 1983 and 1988, the Fourth and Fourteenth Amendments of the United States Constitution, 28 U.S.C. §§ 1331 and 1343(a)(3), the Driver's Privacy Protection Act ("DPPA") 18 U.S.C. § 2721 *et seq.*, and Minnesota common law invasion of privacy.

8. The aforementioned statutory and constitutional provisions confer original jurisdiction of this Court over this matter.

9. This Court has jurisdiction over Kennedy's state law claims pursuant to 28 U.S.C. § 1367.

10. The amount in controversy exceeds $75,000, excluding interests and costs.

The Parties

11. Kirsten Kennedy is, and was at all times material herein, a citizen of the United States and a resident of the State of Minnesota.

12. Defendant City of Braham is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

13. Defendants Entity Does (1-30) are various unknown municipalities as defined by Minn. Stat. § 466.01, subd. 1 that can be sued under Minn. Stat. § 466.01 *et seq*. or other statutes, and federal departments and agencies, which can be sued under 28 U.S.C. § 1346 or other statutes.

14. Kennedy will refer to the entities named in paragraphs 12 to 13 above, along with the Entity Does, collectively as the "Defendant Entities" or "Entity Defendants."

15. Defendant Robert Knowles ("Knowles"), upon information and belief, was, at all times material herein, a citizen of the United States and a resident of the State of Minnesota, duly appointed and acting in his individual capacity as the Chief of the City of Braham Police Department.

16. Defendants John and Jane Does (1-100), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting in their individual capacities as law-enforcement supervisors, officers or employees of the Defendant Entities or other federal, state, county or municipal entities in Minnesota.

17. Kennedy will refer to the individual Defendants (with the exception of the "Commissioner Defendants," "Department of Public Safety Defendants" and "Supervisor Defendants" defined below), including John and Jane Does, collectively as the Individual Defendants" or "Defendant Individuals."

18. Kennedy will refer to the Defendants with supervisory authority over the Individual Defendants, including any John and Jane Does with such supervisory authority, collectively as the "Defendant Supervisors" or "Supervisor Defendants."

19. Defendant Michael Campion ("Campion"), upon information and belief, was, at all times material herein, a citizen of the United States and a resident of the State of Minnesota, duly appointed and acting in his individual capacity as the Commissioner of the Minnesota Department of Public Safety.

20. Defendant Mona Dohman ("Dohman"), upon information and belief, was, at all times material herein, a citizen, of the United States and a resident of the State of Minnesota, duly appointed and acting in her individual capacity as the Commissioner of the Minnesota Department of Public Safety.

21. Kennedy will refer to the Defendants Campion and Dohman collectively, as the "Commissioner Defendants" or "Defendant Commissioners."

22. Defendants DPS Does (1-30), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting their individual capacities as officers, supervisors, employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety.

23. Kennedy will refer to officers, supervisors, employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety who created, installed, monitored, regulated, coded, enforced, supervised, maintained, oversaw, updated, or otherwise worked on the DVS database or BCA database, each of which contained Kennedy's private driver's license information (collectively or individually, "DPS Databases" as "Department of Public Safety Does" or "DPS Does.")

FACTUAL ALLEGATIONS

Defendant Chief Knowles is a Leader of Kennedy's Church

24. Kennedy is a community organizer in North Branch, Minnesota.

25. Kennedy is a clear friend of the police. In her role as a community organizer, Kennedy successfully advocated to help save the North Branch Police Department from closure or reorganization.

26. Kennedy is divorced with five children, living in North Branch, Minnesota.

27. Kennedy is an active participant in her church.

28. Defendant Knowles is the Chief of Police for Braham, Minnesota.

29. Knowles is a leader in the same church, sitting on a council that possesses decision-making authority over congregants. He had knowledge of private information regarding Kennedy's standing in the church.

30. Before 2002, Kennedy counted Knowles's wife as a friend. They attended the same church, their children played together and they socialized with each other.

31. Kennedy and her family left Minnesota from 2002, returning in 2008.

32. Since 2008, Kennedy's only contact with Chief Knowles was church or event related.

33. Kennedy is enrolled in the University of Minnesota-Duluth to obtain a Masters Degree in Advocacy and Political Leadership.

Police Chief Knowles and Other Law Enforcement Officers and Personnel from Entities Across Minnesota Viewed Plaintiffs' Private Information Outside the Scope of Any Investigation or Official Police Business; Knowles Tries to Cover Up His Illegal Actions

34. The Driver and Vehicle Services Division ("DVS") of the DPS maintains a database containing the motor vehicle records of Minnesota drivers. ("DVS Database").

35. The DVS Database contains "personal information" and "highly restricted personal information," as defined by 18 U.S.C. § 2725 ("Private Data"), including but not limited to names, dates of birth, driver's license numbers, addresses, driver's license photos, weights, heights, social security numbers, various health and disability information, and eye colors of Minnesota drivers, both current and former information dating back to the driver's first license issued in Minnesota.

36. The Minnesota Driver's License Application states: "you must provide your Social Security Number…"

37. According to the Minnesota Driver's License Application, "[i]f you don't provide the information requested, DPS cannot issue you a driver's permit, license, or identification card, and your existing driving privileges, may be affected."

38. As early as 2007, Individual Defendants began looking up Kennedy's Private Data on the DVS Database.

39. After the Individual Defendants looked up Kennedy's Private Data, they gained knowledge of the contents of the Private Data. In gaining such knowledge, the Individual Defendants obtained Kennedy's Private Data.

40. Exhibit A, incorporated herein, reflects excerpts of an audit provided by DPS showing each time Kennedy's Private Data was obtained or used by an Individual Defendant.

41. Each act of the Individual Defendants in obtaining Kennedy's Private Data also constituted a disclosure by the Commissioner Defendants, because any release or access of information, whether permitted or not, necessarily requires a disclosure; and the method of setting up the DVS Database and of providing constant access to it constituted a disclosure of Private Data under the DPPA.

42. Column "EsupportStationName" of Exhibit A, incorporated herein, reflect the department or entity which, upon information and belief, employed the Individual Defendant that obtained or used Kennedy's Private Data.

43. Column "EsupportPath" of Exhibit A, incorporated herein, reflect the type of Private Data that was obtained or used by the Individual Defendant.

44. Columns "AccessDay" and "AccessDate," of Exhibit A, incorporated herein, reflect the day of the week, date, and time when the Individual Defendant obtained or used Kennedy's Private Data.

45. DPS does not provide the name of the individual who obtained or used Kennedy's Private Data.

46. Each line of Exhibit A, incorporated herein, reflects the audit of each time Kennedy's information, upon information and belief, was obtained or used by an Individual Defendant without a permissible purpose.

47. Officers employed by, licensed by, or otherwise accessing through the City of Braham obtained Kennedy's Private Data for purposes not permitted by the DPPA forty-nine (49) times.

48. Defendant Braham's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

49. Plaintiff has never been charged with or suspected of committing a crime in the City of Braham, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Braham, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Braham.

50. Rather, Braham's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Braham's personnel.

51. Officers employed by the Entity Defendants, along with those Individual Defendants currently identified as John and Jane Does, obtained or used Kennedy's Private Data approximately seventy-one (71) times.

52. Each of the above accesses was committed knowingly; each of the above accesses was impermissible, meaning that the Defendants had no law-enforcement reason for accessing the information.

53. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers, public employees, or in their job functions.

54. Individual Defendants viewed Kennedy's Private Data from her State-issued driver's license including her home address, color photograph or image, date of birth, eye color, height, weight, medical information, driver identification number, and upon information and belief, social security number.

55. Curiosity about Kennedy or other personal reasons are not purposes permitted for obtaining information under the DPPA.

56. The Individual Defendants mentioned above who made these accesses did so using Kennedy's name, not pursuant to a license plate look-up, and there is seldom any law- enforcement function that would permit accessing Kennedy's private information by name; Kennedy was not involved in any criminal activity nor suspected of any such activity; she had not committed any act that would entitle Entity Defendants and Individual Defendants to access her information under any of the permissible exceptions; to the extent any such permissible reason could exist, Kennedy has eliminated permissible access from the accesses here complained of; and no Defendant has proposed a valid, credible reason for accessing Kennedy's information.

57. Under the direction of the Commissioner Defendants, DPS, and DPS Does, knowingly created the DVS Database that includes Kennedy's Private Data and the system for law-enforcement personnel to access to that information.

58. DPS and DPS Does, under the direction of the Commissioner Defendants, knowingly maintained and updated the DVS Database that included Kennedy's Private Data.

59. DPS Commissioners and DPS Does authored the Minnesota Driver's License Application, which states, "your personal information may be *disclosed* as authorized by United States Code, title 18, section 2721." (emphasis added).

60. DPS Commissioners and DPS Does made the decisions for establishing, ordering the structure of, and determining the persons, agencies and individuals to whom they would disclose the database.

61. The disclosure of information was made by providing a user account and a password without reasonably requiring or ensuring that accesses would be limited to those for a purpose permitted under the DPPA.

62. This form of disclosure was and is used not only for law-enforcement personnel but other recipients who have access to the database, including non-government employees, who comprise about half of the persons who have been granted access to this database.

63. DPS Does and Commissioner Defendants failed to use reasonable care in so disclosing the information in the database.

64. DPS Does and Commissioner Defendants made no reasonable effort nor directed any subordinate to make any reasonable effort to require that the specified purpose of the disclosure was legitimate and would be adhered to by the person to whom the data was disclosed.

65. DPS Does and Commissioner Defendants failed to reasonably ascertain or ensure that the persons to whom it was disclosed would use it permissibly.

66. DPS Does and Commissioner Defendants had at the least constructive knowledge of the widespread abuse of the database by officers illegally accessing it for personal reasons not permitted by the DPPA, and had they not delegated their duties to others would have known of the actual misuse and would have presumably fulfilled their statutory duties and prevented the illegal accesses including those that have adversely affected Kennedy.

67. DPS Does and Commissioner Defendants knowingly disclosed Kennedy's data without requiring that the concomitant access was for a permissible purpose; they disclosed it without taking any effective steps to insure adherence by the individuals—whether private or public sector—accessing it were or would do so for a permissible purpose.

68. Knowledge of the illegal accesses of Kennedy's information by numerous individuals should be imputed to the DPS Does and Commissioner Defendants based in part on their delegation to others of their duty to disclose Private Data for only permissible purposes.

69. DPS Does and Commissioner Defendants failed to ascertain or ensure specifically that law-enforcement personnel would use it permissibly, that is, for a law enforcement function.

70. DPS Does and Commissioner Defendants failed to ascertain or ensure that the persons to whom it was disclosed would use it exclusively for a law-enforcement function.

71. DPS Does and Commissioner Defendants failed to provide adequate training in the permissible uses of the database.

72. DPS Does and Commissioner Defendants, under 18 U.S.C. § 2724(a), knowingly disclosed Kennedy's personal information for a purpose not permitted by the DPPA.

73. DPS Does and Commissioner Defendants gave Individual Defendants access to the database for purposes of their intended misuse of the database.

74. Disclosure of this database is a matter known to and participated in and directed by the DPS Does and Commissioner Defendants.

75. The DPS Does and Commissioner Defendants had a duty to ascertain the recipients' purpose for his/her obtainment or use of the private data.

76. The DPS Does and Commissioner Defendants, at times, delegated the duty to ascertain the recipients' purpose to other individuals.

77. To the extent the DPS Does and Commissioner Defendants delegated any part of their duties, they are still responsible for disclosure and ascertainment of purpose, and the persons, to whom they may have delegated, if any, are not known to Kennedy and cannot be known by Kennedy.

78. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2007.

79. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2008.

80. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2009.

81. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2010.

82. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2011.

83. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2012.

84. DPS Does and Commissioner Defendants continue to fail to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2013.

85. DPS and DPS Does, under the direction of Commissioner Defendants, had the ability to determine that drivers' license information, including Kennedy's Private Data, was being accessed on multiple occasions, by multiple law-enforcement personnel from multiple law-enforcement agencies.

86. DPS and DPS Does, under the direction of the Commissioner Defendants, had the ability to prevent unauthorized access to the DVS Database, including unauthorized access to Kennedy's Private Data.

87. DPS and DPS Does, under the direction of the Commissioner Defendants, failed to prevent unauthorized access to the DVS Database, including access to Kennedy's Private Data.

88. The Commissioner Defendants and DPS Does knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in the disclosure of Kennedy's Private Data.

89. The policy of the State of Minnesota is to uphold the provisions of the law, both state and federal, and to protect and safeguard the privacy rights of the State's citizens and inhabitants, including its drivers' privacy rights, and including those rights as are required to be protected by federal law.

90. In particular, it is the policy of the State of Minnesota, as outlined in Minn. Stat. § 171.12, subd. 7, to comply with the provisions and requirements of the DPPA.

91. This policy is also set forth in the driver's license application and set forth in statutory language with proper citation to that federal statute.

92. Defendant Commissioners and DPS Does knowingly disclosed Kennedy's and others' Private Data and violated state policy by devising and implementing a database, such as the DVS Database, that failed abysmally to uphold the privacy rights of Kennedy and others similarly situated as protected by the DPPA.

93. This failure exposed their information to impermissible and knowing accesses by various persons, including the Defendants in this lawsuit.

94. These acts and failures to act by Defendant Commissioners and DPS Does constitute knowing disclosures of Kennedy's information within the meaning of the DPPA.

95. Defendant Commissioners and DPS Does knowingly devised and implemented a database and a method for using and misusing that database that both permitted and encouraged, through the nature and monitoring of the system, accesses by law-enforcement personnel, state employees, and others that failed to comply with state policy of protecting privacy rights and complying with the DPPA.

96. The system knowingly devised and implemented by Commissioner Defendants and DPS Does failed to set rules protecting Kennedy's privacy rights.

97. This system permitted, and on information and belief still permits, the accessing of the database from personal computers.

98. This system allowed individuals to give out their personal passwords to others.

99. This system permitted, and on information and belief may still permit, the accessing of the system by persons without any accountability or even in some instances without the ability to trace the person who made the access.

100. From 2003 through 2010, this system did not require reasonably adequate training on the use of the DVS database of sworn-law enforcement officers.

101. From 2011 through today, this system still does not require reasonably adequate training on the use of the DVS database of sworn law-enforcement officers.

102. Accordingly, the effective monitoring of the system is difficult if not impossible under the system as devised and implemented by Commissioner Defendants and DPS Does.

103. Commissioner Defendants and DPS Does have deliberately emphasized and favored the convenience of the system by users at the expense of protecting the privacy rights of the persons whose information is in the database.

104. This deliberate emphasis and preference for convenience to the system users over the privacy rights of the drivers was known to the Commissioner Defendants and the DPS Does, and was purposeful.

105. In failing to properly implement, maintain, and monitor the DVS Database, Commissioner Defendants failed to follow Minnesota state policy.

106. Many viable methods were and are available to prevent this illegal accessing of private information.

107. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were accessing the databases for purposes not permitted under the DPPA.

108. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were viewing Kennedy's Private Data without a legitimate and permissible purpose.

109. Upon information and belief, the Commissioners and DPS Does acquiesced, facilitated, approved, or simply ignored the improper conduct by governmental personnel.

110. Even if the Commissioners and DPS Does had no actual knowledge of the impermissible uses of the databases they oversaw, upon information and belief, they were reckless in their supervision of their subordinates who did operate the database.

111. Upon information and belief, the Commissioners and DPS Does were negligent in supervising their subordinates who operated the databases.

112. The information contained in the DPS database is far greater and contains more private personal information than is customarily known to non-law enforcement personnel.

113. The information contained in the DPS database includes the social security numbers of the drivers, including Kennedy's social security number.

114. The information contained in the DPS database includes drivers' health information, including Kennedy's medical information.

115. These accesses are committed surreptitiously, and without the knowledge of the victims, including Kennedy, which knowledge is kept hidden and concealed from the victims, including Kennedy.

116. There has not been a single instance of which Kennedy is aware involving her or anyone else where an officer has informed her that he or she has accessed her information, except for Defendant Knowles in 2013, as described below.

117. Law-enforcement officers have gone to great lengths to avoid letting Kennedy know they have accessed her personal private information.

118. The surreptitious, concealed, and hidden accesses are kept secret from the general public and from the victims, including Kennedy.

119. Paradoxically, the practice of impermissibly viewing drivers' private information on the DVS Database and BCA Database is well known throughout the law-enforcement community, from top ranking officers to the lowest ranking personnel.

120. Commissioner Defendants and DPS Does allowed multiple breaches of the security of Kennedy's Private Data in violation of Minn. Stat. 13.055.

121. Commissioner Defendants and DPS Does failed to disclose to Kennedy this breach of the security of the data in violation of Minn. Stat. 13.055.

122. Obtaining the DVS Database without a permissible reason is a breach of confidentiality.

123. Kennedy contacted DPS to inquire whether law-enforcement officers had been viewing her private information.

124. The DPS website states that the public is entitled to information except that which is classified:

> [T]he law states that all the data DPS or a governmental entity has are public (can be seen by anybody) unless there is a state or federal law that classified the data as not public. You have the right to look at all public data that DPS keeps.
>
> (*See* "Minnesota Department of Public Safety: Public Access to Government Data," attached to this Complaint as Exhibit B)

125. The DPS website also informs the public that anyone can request information in any way, by phone, in person, mail, or email; that specific data can be requested, or "entire records, files or data bases" or all public data that DPS keeps." It instructs the person requesting the information that "you don't have to tell us who you are or explain why you are asking for the data." *Id*.

126. But despite its stated policy, before August 2011, the actual practice of DPS was to withhold, deny and mislead the public to prevent access to this information. (*See* Affidavit of Dan Prozinski and attached exhibit, attached to this Complaint as Exhibit C; August 23, 2011 email from Joseph Newton to A. Geraghty, attached to this Complaint as Exhibit D (DPS attorney, Newton wrote, "[w]e generally need more than a bald allegation, does she have anything more to base her allegations?"; and the Second Amended Complaint to *Kampschroer v. Anoka Cty., et. al*, 13-2512 SRN/TNL, at ¶¶ 410 – 426).

127. DPS practice in this regard amounted to concealment of the illegality, by misleading the public on those occasions when they became suspicions about the invasion of their private data.

128. These invasions or illegal accesses of her Private Data were by their very nature actively concealed, since those making the accesses concealed them from their supervisors and from Kennedy; at no time did anyone approach Kennedy and advise her that he or she had accessed her Private Data, except as alleged for Knowles, below.

129. In 2013, Plaintiff requested an audit from Kim Jacobson at DPS.

130. The Minnesota Department of Motor Vehicles is a division of DPS.

131. After requesting, but before receiving the audit, Kennedy saw Defendant Knowles at a graduation party for Chief Knowles nephew.

132. She mentioned to him that she had requested the audit and said, "have you ever heard of people looking at driver's licenses?"

133. Kennedy asked Chief Knowles whether it was okay for law enforcement to look at her private information/

134. Chief Knowles replied, "it would not be allowed or legal."

135. When Kennedy was leaving the graduation party, Chief Knowles casually said, "I've looked you up a couple of times."

136. Again, after Kennedy had requested the audit, but before she received it, Chief Knowles called Kennedy.

137. In this unexpected phone call, Chief Knowles again told Kennedy that his name was going to appear in the audit.

138. Chief Knowles added, "let's be clear, you asked me to look you up and it was four times?"

139. Kennedy had never asked Chief Knowles to look up her Private Data.

140. Kennedy found Chief Knowles' unsolicited call extremely unsettling.

141. On June 5, 2013, Jacobson provided the results of the audit to Kennedy.

142. The audit request and the results furnished, were for name look-ups only and specifically did not include any license plate or driver's license number look-ups.

143. Kennedy was sickened to learn from DPS that it had determined that officers and personnel from approximately several different departments and agencies had reviewed, and impermissibly obtained or used, her Private Data approximately 71 times since 2007. *See* Exhibit A.

144. The audit indicates that personnel from the City of Braham obtained Kennedy's Private Data 49 times from 2009 through 2012.

145. On or about June 3, 2013, Sally Hoy, the Chief Administrator of the City of Braham sent a letter to Kennedy.

146. In the letter, Hoy acknowledged that only one Braham police officer had obtained Kennedy's data 49 times.

147. Hoy related in the letter that she had a conversation with Chief Knowles about his use of the database. Chief Knowles acknowledged that the only person he queried that much was Kennedy.

148. According to Hoy, Chief Knowles said that "Kennedy was a friend to him and his wife, and that [Kennedy] had requested him to keep an eye on [her] driver's license record to make sure nothing was on it . . ."

149. As noted above, Kennedy considered Knowles' wife a friend, but did not consider that she had a friend-type of relationship with Knowles.

150. More significantly, it is simply untrue that Kennedy requested that Chief Knowles check her driver's license record. She never did anything of the sort.

151. Kennedy never authorized or consented to Chief Knowles' reviewing or obtaining her driver's license information.

152. Kennedy had never asked Knowles to look her up, not once, not four times, and not 48 times.

153. Rather, Chief Knowles was trying to cover up his illegal actions to his employer.

154. Chief Knowles tried to cover it up when he called Kennedy at her home, further imposing on her privacy and falsely said he had obtained her information only four times and with her permission.

155. Chief Knowles persisted in minimizing and concealing his conduct by misleading the Braham City Administrator about the nature of his relationship with Kennedy and the purpose of his conduct.

156. Before requesting the audit report, Kennedy had no knowledge that her Private Data had been obtained through the DVS Database.

157. Plaintiff was not under any criminal investigation; she had committed no crimes; she was not seeking the assistance of law-enforcement; she was not a witness to any crime, nor was she involved with anyone in a criminal investigation, or even a civil lawsuit; she was not of any legitimate interest to law-enforcement other than for personal reasons, such as curiosity or romantic attraction.

158. There is no possible law-enforcement function that would have made invading Plaintiff's privacy permissible under the DPPA.

159. Before filing suit, Plaintiff (through her attorneys) contacted the Entity Defendants, providing the relevant portion of the audit, sending them a letter in which she requested the Entity to provide her with any permissible reason it or its employees, agents, and officers had in looking up her information; Defendants never provided any legitimate permissible reason for these illegal accesses..

160. Kennedy believes that even more unauthorized accesses and viewings will occur in the future if the policies of Entity Defendants and other police departments and law-enforcement agencies similarly situated are not changed to bring the actual custom and practice of these Entity Defendants and others similarly situated into compliance with their own written rules, with the rules of the Department of Public Safety, and with federal law, including the DPPA.

161. Included in the audit is the listing of various law-enforcement departments associated with the Defendant Entities that obtained Kennedy's Private Data.

162. Individual Defendants' identities (John and Jane Does) are not presently known, and purportedly cannot be revealed pursuant to the Minnesota Government Data Practices Act. Kennedy anticipates that these yet-to-be-named Individual Defendants will become known through discovery.

163. Supervisor Defendants are not presently known. Kennedy anticipates that the yet-to-be-named Supervisor Defendants who should have monitored, prevented and

stopped the unauthorized accesses to Kennedy's information will become known through discovery.

164. The remaining Entity Defendant identities (Entity Does) are not presently known, because not all of the entities identified by the DPS have provided sufficient information to determine if their personnel's access to the database was unauthorized. Kennedy anticipates that these yet-to-be-named Entity Defendants will become known through discovery.

165. Defendant Commissioners released and disclosed this information without training or with wholly inadequate training for the individuals with access to the DVS database.

166. Defendant Commissioners released and disclosed Kennedy's Private Data to individuals without ascertaining whether it was obtained for a purpose permitted under the DPPA, but instead relied on the status of the person obtaining it, assuming that because of the person's status their obtainment of the information was for a purpose permitted by the DPPA.

167. Whatever training, monitoring, or inquiry into the officers' usage of the information systems has been adopted is woefully inadequate to ensure that access is used properly and lawfully.

168. On information and belief, despite this training, Defendant Entities and Defendant Supervisors, allowed their employees, including but not limited to Individual Defendants, to view Kennedy's Private Data for unlawful purposes.

169. On information and belief, Defendant Entities, Defendant Supervisors, and Commissioner Defendants permitted, condoned, or acquiesced in this illegal access to Kennedy's private information, and knew or should have known that it was occurring.

170. On information and belief, this illegal access occurs with regularity not only of Kennedy's private information, but of other Minnesota drivers' private information.

171. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does have lax policies or lax enforcement of these policies that allow for these intrusions.

172. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal access to individuals' private information by their officers.

173. The Driver's License application assures Minnesota drivers their information will be safeguarded and kept private, "DPS releases this information to local, state, and federal government agencies only as authorized or required by state and federal law."

174. Kennedy submitted her Private Data to DPS, including her social security number, because of the promise of confidentiality made by DPS.

175. Kennedy relied on this promise of confidentiality when she provided her Private Data to DPS to obtain a driver's license.

176. The failure of Defendant Entities and Defendant Supervisors to keep this information private is a flagrant breach of a promise of confidentiality.

177. Defendant Entities, Defendant Supervisors, Commissioner Defendants, and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal access to individuals' private information by their officers.

178. The extent of this illegal access is widespread and pervasive throughout departments, and is a custom and practice.

179. The widespread practice is demonstrated by the systematic tolerance of illegal accesses.

180. Further evidence of the custom and practice can be found in actual statements made by current officers, one of whom was quoted in a magazine article about the illegal access into previous cases involving this same breach of privacy as saying that "every single cop in the state has done this. Chiefs on down."

181. Further evidence is based on actual statements made by former officers, one of whom was quoted in a magazine article about illegal accesses of other individuals as saying that "[y]ou used to look up people without a second thought. You'd look up old friends from high school or just someone you used to know."

182. Each individual with access to the DPS Database has a password allowing that individual access to the DPS Database.

183. Personnel can access the DPS Databases from any computer with internet access.

184. Personnel occasionally gave other individuals their passwords, contrary to requirements.

185. The system for accessing accountability and responsibility was and is prone to error and fails to reasonably protect drivers' private information.

186. When Defendant personnel viewed Kennedy's private information, they did not do so to carry out official police functions.

187. Kennedy committed no crimes or transgressions that would explain or legitimize the unauthorized access of their Private Data.

188. The Individual Defendants obtained Kennedy's personal information without probable cause or reasonable suspicion to believe that Kennedy had engaged in any criminal activity or any activity even remotely related to criminal activity.

189. Kennedy never waived the protections of the DPPA.

190. Defendants' actions have violated the United States Constitution, the DPPA, 42 U.S.C. § 1983, and Minnesota State law.

191. The sheer volume of the intrusions into her private life demonstrates that law-enforcement personnel, public employees, and others are unfairly hostile and careless toward Kennedy's privacy and safety.

192. As a result of these invasions of privacy, Kennedy has suffered and continues to suffer emotional distress.

193. Receiving Chief Knowles unsolicited call, learning about the extent of his access into her private life and about his attempts to cover his tracks made Kennedy sick to her stomach.

194. She believed that as a leader of her church, and as a leader of local law enforcement, Chief Knowles' function was supposed to be to protect her rights, instead, he has been acting like a Peeping Tom, spying on her private life.

195. By falsely claiming that Kennedy had asked him to obtain her Private Data, Chief Knowles is blaming the victim for his own illegal actions.

196. Chief Knowles' behavior has emotionally distressed and disturbed Kennedy and continues to do so.

THE COMMISSIONERS HAVE KNOWN ABOUT THESE VIOLATIONS

197. DPS Commissioners Campion and Dohman have been involved with law enforcement for many years.

198. Commissioner Dohman has been a law enforcement officer for thirty years, having formerly served as police chief of the City of Maple Grove from 2001 until her appointment as DPS Commissioner in March 2011.

199. Before becoming Chief of Police of the Maple Grove Police Department she was an investigator, patrol officer, sergeant and captain of the Maple Grove Police Department; and prior to that time, she was a patrol officer of the City of Glencoe and of the City of Marshall, Minnesota.

200. Dohman also served as president of the Minnesota Chiefs of Police Association.

201. Upon information and belief, the misuse of private information is the main complaint of most police chiefs and human resources personnel.

202. Former Commissioner Michael Campion served from July 2004 until March 2011. Prior to his appointment as DPS Commissioner he was supervisor of the BCA, which also maintains a driver's license database.

203. Prior to that position, Campion was a special agent at the BCA.

204. It was during his tenure that the DPS database was largely developed in its current format.

205. On information and belief, misuse of the DPS database has been well-known to Commissioner Defendants. At a Legislative Audit Subcommittee hearing in February, 2013 at which Commissioner Dohman testified, the testimony of the Legislative Auditor revealed that at least 50% of law enforcement officers are misusing the DPS database by obtaining, disclosing, and/or using the driver license personal information for an impermissible purpose.

206. On information and belief, Commissioner Defendants knew this, and knowingly disclosed the information in part by (a) failing to safeguard and monitor the database despite knowing of its rampant misuse, (b) willfully refusing to correct the misuses, or (c) both failing to monitor and refusing to correct the abuse and misuse of the system.

207. Experts in the field of police training report that the primary complaint of many police departments is that law enforcement personnel misuse private information. This is an established, well-known, and pervasive problem with law enforcement that Commissioner Defendants are unwilling to properly address.

THE COMMISSIONER DEFENDANTS AND DPS DOES REASONABLY COULD HAVE DONE SIGNIFICANTLY MORE TO PROTECT KENNEDY'S PRIVACY.

208. On information and belief, the only changes and improvements to the DPS system to increase the protection of privacy, especially from law enforcement, have occurred only after litigation involving DPS, specifically the lawsuit titled Anne Marie Rasmusson v. City of Bloomington, No. 12-CV-00632 (SRN/JSM). In that case Plaintiff sued, among others, the Commissioners of the DPS and was able to obtain through settlement significant changed to the DVS database, including numerous protections such as different types of periodic audits. On information and belief, the 19,000 improper accesses of former Department of Natural Resources Captain John Hunt were discovered in part due to those changes. The vast majority of the restrictions and protections on driver privacy have occurred due to the Rasmusson case and others like it. The Commissioners in Minnesota remain highly resistant to improving the DPS database, instead looking to the individual officers and local governments to institute changes, which is a far less effective method of instituting changes and will result in piecemeal and inadequate changes in protections at best.

209. On information and belief, states other than Minnesota have far greater restrictions and protections in place to protect the data on their drivers' license databases from being obtained, disclosed or used for a reason not permitted by the DPPA.

210. For instance, on further information and belief, North Dakota requires a daily report of anyone who obtains driver photos and its system generates weekly reports listing all individuals with accesses of over 25 images a day. These reports are sent to the

North Dakota Attorney General to make inquiries as to whether the information was obtained for a job-related reason. North Dakota also requires the users of the database to declare the reason why they were looking at the record. North Dakota also requires its users to take a certification test before being given access to the database.

211. Also on information and belief, the State of California's DMV cooperates with its law-enforcement agencies and California's Department of Justice to ensure access to its drivers' license information is limited to agencies that satisfy specific requirements before they are issued a confidential requester code that permits access to law-enforcement information only. Each law-enforcement agency is responsible for limiting access to necessary personnel. California also periodically reviews law-enforcement applications to ensure the agency and person requesting the information is still entitled to obtain the information. During a recent audit, California's DMV reviewed questionable agencies and even reclassified some to prevent them from having further access to the database.

212. On further information and belief, the California DMV has a dedicated law-enforcement unit to analyze data inquiries. Each data request is logged and technicians are trained to look for developing patterns in the requester's history. The California DMV also conducts periodic historical reviews of a specific agency's requests to determine if the accesses were authorized. The California DMV may also require a law-enforcement entity to supply an explanation of events, describe their protocols for accessing DMV information, what policies or access requirements were violated, what corrective or administrative steps are being taken to admonish the officer, and what steps

the agency is taking to avoid future occurrences. All users annually complete an information security form. Finally, the California DMV is very restrictive on the types of information it releases.

213. On information and belief, DPS Commissioners, DPS and Defendants Entities knew or should have known of the policies and practices of other States, but did not a the time that Kennedy's drivers' license information was being impermissibly obtained, require any of the protections and safeguards to the Minnesota DPS Databases utilized by other states.

214. Given that other states do and did have safeguards and protections in place to protect their drivers' private information from impermissible accessing, use, and disclosure, DPS Commissioners, DPS and Defendants Entities reasonably should have implemented such safeguards and protections for Minnesota drivers, including Kennedy.

215. The implementation of some or all of these safeguards and protections by Defendants would have prevented many of the impermissible obtainment, uses, and disclosures of Kennedy's private data.

COUNT I: VIOLATION OF THE DPPA, 18 U.S.C. § 2721, *et seq.*

(Against all Defendants)

216. Kennedy reaffirms and realleges the allegations in Paragraphs 1 through 215.

217. Kennedy provided personal information to the DPS including her address, color photograph, date of birth, weight, height, eye color, social security number and

medical information for the purpose of acquiring and utilizing a State of Minnesota driver's license.

218. The DPS Database also maintained Kennedy's driving record.

219. Kennedy did not provide her consent for any of Defendant Individuals to obtain, disclose or use, or for any of Defendant Entities or Defendant Supervisors to disclose or to allow Defendant Individuals to obtain, disclose or use, her private information for anything but official law-enforcement business.

220. Knowingly obtaining, disclosing or using Private Data for a purpose not permitted by the DPPA is a violation of the DPPA. The statute provides for criminal fines and civil penalties. 18 U.S.C. §§ 2723, 2724.

221. The DPPA provides redress for violations of a person's protected interest in the privacy of their motor vehicle records and the identifying information therein.

222. Minnesota law is to enforce and follow the DPPA and to hold all information obtained pursuant to an application for a driver's license confidential and private; even prior to the passage of the DPPA in 1994 Minnesota law pledged to hold all this information private and confidential, and on one's driver's license application these promises of confidentiality are all made; Defendants' actions in accessing this information is a flagrant breach of that pledge of confidentiality.

223. Each of the Defendants invaded Kennedy's legally protected interest under the DPPA.

224. According to the Department of Vehicle Services, the Individual Defendants knowingly obtained, disclosed or used Kennedy's personal information, from

a motor vehicle record, for a purpose not permitted under the DPPA. 18 U.S.C. § 2724(a).

225. None of the Individual Defendants' activities fell within the DPPA's permitted exceptions for procurement of Kennedy's private information.

226. By the actions described above, each Defendant Individual was acting within the scope of his or her employment when he or she obtained, disclosed or used Kennedy's personal information from the DPS Databases for a purpose not permitted by the DPPA.

227. Individual Defendants knew that their actions related to Kennedy's Private Data were in violation of the DPPA.

228. Defendant Entities and Defendant Supervisors knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in obtaining, disclosing or using of Kennedy's private personal information by Individual Defendants.

229. Defendant Commissioners, Defendant Entities and Defendant Supervisors' actions constitute a knowing disclosure of the personal information of Kennedy under the DPPA.

230. Individual Defendants knowingly used Defendant Entities' computers, passwords and passcodes to obtain Kennedy's private information.

231. Kennedy's private information was obtained by each Individual Defendant for purposes that are not permitted under the DPPA.

232. Chief Knowles knowingly obtained Kennedy's private information 49 times for purposes not permitted by the DPPA.

233. Chief Knowles tried to coerce Kennedy to back his untrue story about the reasons for his abuse of the DPS database.

234. Chief Knowles tried to mislead the City of Braham about the purpose of his obtaining Kennedy's private information.

235. Defendant Entities are each vicariously liable for the acts of Defendant Individuals.

236. By the actions complained of, Commissioner Defendants, and DPS Does are jointly liable for the acts of Defendant Individuals.

237. Kennedy has suffered harm because her private information has been obtained and viewed unlawfully.

238. Kennedy has further suffered harm because her private information has been obtained unlawfully. Kennedy suffered and continues to suffer harm by virtue of the increased risk that her protected information is in the possession of Individual Defendants who obtained it without a legitimate purpose.

239. This is precisely the harm Congress sought to prevent by enacting the DPPA and its statutory remedies.

240. Individual Defendants, Supervisor Defendants, and Commissioner Defendants each willfully and recklessly disregarded the law, entitling Kennedy to punitive damages under the DPPA, see 18 U.S.C. § 2724(b)(2), which is not subject to the pleading requirement of Minnesota state law as set forth in Minn. Stat. § 549.20. Kennedy is entitled to actual damages, punitive damages, reasonable attorneys' fees and

other litigation costs reasonably incurred, and such other preliminary and equitable relief as the court determines to be appropriate. 18 U.S.C. § 2724(b).

241. In addition, under the DPPA, Kennedy is entitled to a baseline liquidated damages award of at least $2,500 for each violation of the DPPA. 18 U.S.C. § 2721(b)(1). Kennedy need not prove actual damages to receive said liquidated damages.

COUNT II: VIOLATION OF 42 U.S.C. § 1983

(Against All Individual Defendants Including Chief Knowles and Jane and John Does)

242. Kennedy reaffirms and realleges the allegations in Paragraphs 1 through 241.

243. The Fourth Amendment to the Constitution of the United States provides for the right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

244. The Fourteenth Amendment provides all individuals in the United States with a substantive due process right of privacy.

245. The Fourth Amendment to the Constitution of the United States establishes a well-settled civil right to be free from an unconstitutional search.

246. At no time did Kennedy behave in a manner that would provide any legal justification for the above-described invasion of her privacy.

247. The DPPA establishes that obtaining an individual's Private Data without a legitimate purpose constitutes an illegal search under the meaning of the Fourth Amendment as well as a violation of their substantive due process right to privacy under the Fourteenth Amendment.

248. The DPPA, among other things, such as the plain language of the Constitution, the various court decisions interpreting the Constitution and the traditions of our country establish that an individual has a reasonable expectation of privacy in their driver's license information.

249. Individual Defendants' viewing of Kennedy's personal information was unauthorized, unjustified, and excessive, and violates the Fourth and Fourteenth Amendments, the laws of the United States and the laws of the State of Minnesota.

250. By the actions described above, each Individual Defendant, acting under color of state and federal law, violated and deprived Kennedy of her Fourth and Fourteenth Amendment Rights.

251. Individual Defendants used the Entity Defendants' computers, passwords and passcodes to obtain Kennedy's Private Data.

252. The acts of each Individual Defendant, acting under the color of state and federal law, constituted an invasion or repeated invasions of Kennedy's clearly-established privacy rights, guaranteed by the Bill of Rights and the Fourteenth Amendment to the United States Constitution, the laws of the United States, including the DPPA, and the laws of the State of Minnesota.

253. The DPPA protects and codifies an individual right to privacy in a person's Private Data, thereby prohibiting unauthorized accessing of all persons' information, including Kennedy's information.

254. Each individual law-enforcement and other government personnel, acting under color of state and federal law, knew that his or her actions violated and deprived Kennedy of her clearly established statutory rights under the DPPA.

255. Each Individual Defendant deprived Kennedy of her federal statutory rights and civil rights maliciously or by acting with reckless disregard for whether Kennedy's rights would be violated by his or her actions.

256. Each Individual Defendant was deliberately indifferent to Kennedy's statutory and civil right to be free from illegal searches, invasions of privacy and the unauthorized accessing of their Private Data.

257. As a direct and proximate result of the acts and omissions of the above-named Individual Defendants, Kennedy was damaged in an amount yet to determined, but in excess of $75,000.

258. Punitive damages are available against Individual Defendants for their reckless and callous disregard for Kennedy's rights and their intentional violations of the federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirement for punitive damages set forth in Minn. Stat. § 549.20.

259. Kennedy is entitled to recovery of her costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT III: VIOLATION OF 42 U.S.C. § 1983

(Against Entity Defendants and Supervisor Defendants, including John, Jane and Entity Does, for violation of 42 U.S.C. § 1983)

260. Kennedy reaffirms and realleges the allegations in Paragraphs 1 through Paragraph 259.

261. Individual Defendants' numerous accesses of Kennedy's private information are not unique, but one example of how frequently such law-enforcement agencies and other governmental entities customarily violate the DPPA by accessing Private Data of persons without having any legitimate or permissible reason for doing so.

262. Persons familiar with police departments and those involved in teaching supervisors how to train and hold accountable their subordinate law-enforcement personnel have been told by those supervisors that the unlawful and impermissible accessing of private information is among the most frequently committed wrongs by police, for which they are seldom if ever held accountable.

263. Improper access of citizens' Private Data by Defendants for their own personal and private uses, obtained by accessing that information through the computerized information storage system kept by the State for official purposes only, is an official custom or practice well known to Defendant Supervisors and Commissioner Defendants.

264. These customs and practices by Defendant Individuals are at variance with the written rules set down by the Entity Defendants, the DPS, and Commissioner Defendants, but these formal rules are widely and knowingly disregarded.

265. Given Entity Defendants' failure to monitor and enforce their rules, the aforementioned customs and practices are attributable to the municipalities themselves, including the Entity Defendants herein.

266. Defendant Entities and Defendant Supervisors of the law-enforcement personnel and other public employees accessing this information knew or should have known of this and other unlawful, improper, unjustified, and impermissible access to private information by law-enforcement personnel and other public employees.

267. The prevalence of this custom, the lack of monitoring regarding these access practices and the failure to take action to stop or prevent these practices, demonstrate the state of mind of Defendant Supervisors and municipal officials of the Entity Defendants.

268. These customs and practices further demonstrate Defendants' deliberate indifference to the federal statutory and constitutional rights of the citizens and persons, including Plaintiff, whose information has been wrongfully accessed.

269. Defendant Entities are directly liable for the custom and practice of the widespread illegal access of citizens' Private Data.

270. Supervisor Defendants, up to and including the chief police officers and sheriffs employed by each Entity Defendant, are liable in their individual capacity.

271. Defendants' liability is due to their actual and constructive knowledge of this practice.

272. Defendants' liability is also due to their failure to institute any process for monitoring and preventing it.

273. Defendants' liability is also due to their deliberate indifference to the federal rights of those persons, including Kennedy, whose information has been and continues to be wrongfully accessed.

274. In addition, Defendant Supervisors of the law-enforcement personnel and other public employees, up to and including the chief police officer in each of Defendant Entities, are liable in their individual capacities for the failure to train, monitor, supervise, and properly discipline the officers who are improperly and unlawfully accessing the Private Data of citizens, including Kennedy, without a proper, lawful, permissible, justifiable purpose for doing so.

275. This pattern of failure to train, monitor, supervise, and discipline demonstrates the state of mind of these Defendant Supervisors and a deliberate indifference to the rights of the citizens and others whose information has been so widely accessed, including Kennedy.

276. The federal rights of the citizens, including Kennedy, whose information was improperly accessed, are held in light regard by many if not most of the Defendant Supervisors and by the Defendant Entities themselves.

277. Defendants' lack of concern evidences their deliberate indifference both to the problem of the unauthorized access and to the impact of the unauthorized access on the federal rights of the citizens, including Kennedy, who would often be unaware of that access.

278. It is yet unknown whether a system has been established by the Entity Defendants and Supervisor Defendants to monitor the regular access of the DPS Databases by personnel.

279. It is yet unknown whether any attempt has been made by Entity Defendants and Supervisor Defendants to provide redress and assurance to the persons, including

Kennedy, whose DVS information has been wrongfully accessed by the Individual Defendants named in this Complaint, or by other personnel in the municipalities named in this Complaint.

280. As a direct and proximate result of the acts and omissions of the above-named Defendant Entities and Defendant Supervisors, Kennedy has endured and continues to endure mental suffering, and has been damaged in an amount yet to be determined and of a continuing nature, but in an amount in excess of $75,000.

281. Punitive damages are available against Defendant Supervisors for their reckless and callous disregard for Kennedy's rights and their intentional violations of the federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirements set forth in Minn. Stat. § 549.20.

282. Kennedy is entitled to recovery of her costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT IV: VIOLATION OF 42 U.S.C. § 1983

(Against Commissioner Defendants and DPS Does)

283. Kennedy reaffirms and realleges the allegations in Paragraphs 1 through 282.

284. As DPS Commissioners, Campion and Dohman, along DPS Does, were and are responsible for creating, maintaining, and providing access to the database that included Kennedy's Private Data.

285. Defendant Commissioners and DPS Does also had the ability to determine if unauthorized access was being made and to prevent such unauthorized access to the database, including of Kennedy's Private Data, and have the ongoing duty to prevent such unauthorized accesses.

286. Defendant Commissioners and DPS Does failed to utilize any due care to ensure that the disclosed information was being used only for permissible purposes.

287. Commissioner Defendants and DPS Does failed to prevent unauthorized access to the database, including Kennedy's Private Data.

288. The actions of Commissioner Defendants and DPS Does, as alleged, violate the rights of Kennedy under the Fourth and Fourteenth Amendments to the United States Constitution and under the DPPA.

289. On information and belief, Commissioner Defendants, and DPS Does created or oversaw the creation and maintenance of a database and system that was supposed to prevent unauthorized access to Private Data.

290. From 2007, Commissioner Defendants and DPS Does allowed unauthorized access of Kennedy's Private Data about 71 times.

291. On information and belief, Commissioner Defendants' and DPS Does' efforts have been insufficient to prevent future unauthorized access of Kennedy's and other individuals' private, personal information.

292. Commissioner Defendants and DPS Does have sanctioned the constitutional violations by the Individual Defendants through their failure to remedy the

policy, custom and practice of officers' and employees' unfettered and unauthorized access to the database.

293. Commissioner Defendants and DPS Does have been negligent in supervising subordinates responsible for implementing a law-enforcement database that prevents unauthorized access to private, personal information.

294. On information and belief, Commissioner Defendants and DPS Does failed to monitor and prevent unauthorized access to private, personal information even though they knew or should have known that such unconstitutional acts were occurring.

295. Commissioner Defendants and DPS Does, acting under the color of state law, were deliberately indifferent to Kennedy's constitutionally-recognized and federal statutory rights to be free from illegal searches, invasions of privacy and the unauthorized accessing of her Private Data.

296. Commissioner Defendants and DPS Does failed to implement properly Minnesota's policy to protect the private, personal information of its citizens with drivers' licenses.

297. Commissioner Defendants and DPS Does are jointly liable for the use, disclosure, or access of Kennedy's Private Data for each Individual Defendants' access.

298. As a direct and proximate result of the acts and omissions of Commissioner Defendants and DPS Does, Kennedy was forced to endure physical and mental suffering, and was thereby damaged in an amount yet to determined, but in an amount in excess of $75,000.

299. Punitive damages are available against Commissioner Defendants and DPS Does for their reckless and callous disregard for Kennedy's' rights and their intentional violations of the federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirements set forth in Minn. Stat. § 549.20.

300. Kennedy is entitled to recovery of her costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT IV: COMMON LAW INVASION OF PRIVACY

(Against All Defendants)

301. Kennedy reaffirms and realleges the allegations in Paragraphs 1 through 300.

302. By improperly obtaining Kennedy's private personal information for impermissible reasons, Defendants intentionally intruded upon the solitude or seclusion of Kennedy's private affairs and concerns.

303. Chief Knowles intruded on the seclusion of Kennedy's private affairs and concerns by obtaining her data without permission 49 times, and calling her at home to coerce her to help him cover it up.

304. Defendants' intrusions would be highly offensive to a reasonable person.

305. Defendants' intrusions caused Kennedy to suffer severe emotional distress and physical harm.

306. Defendants' intrusions were intended to cause Kennedy to suffer severe emotional distress and physical harm, and was made with either actual or legal malice, or with reckless disregard of her rights and her privacy.

307. Kennedy is entitled to tort damages for Defendants' invasion of privacy.

JURY DEMAND

308. Kennedy demands a jury trial as to all issues of fact herein properly triable to a jury under any statute or under common law.

WHEREFORE, Kirsten Kennedy prays for judgment against the Defendants as follows:

1. A money judgment against all Defendants for liquidated, actual and compensatory damages in an amount in excess of seventy five thousand ($75,000) dollars and punitive damages in an amount to be determined by the jury, together with their costs, including reasonable attorney fees, under 42 U.S.C. § 1988, the DPPA, and other applicable laws, and prejudgment interest;

2. Actual damages, punitive damages, attorneys' fees and other litigation costs and such other preliminary and equitable relief as the court determines to be appropriate under 18 U.S.C. § 2724(b);

3. Liquidated damages of at least $2,500 for each violation of the DPPA under 18 U.S.C. § 2721(b)(1);

4. An injunction, permanently enjoining all Defendants from viewing Kennedy's private information in violation of the DPPA, unless necessary for law enforcement purposes;

5. An injunction, permanently and prospectively requiring Defendants to establish and implement all effective monitoring and investigative procedures to end this practice, discover and suspend permanently all accessing privileges to the violators; and to provide full disclosure to all potential claimants of the entities and persons who have violated their rights under the DPPA and the Constitution; and,

6. For such other and further relief as this Court deems just and equitable.

SAPIENTIA LAW GROUP PLLC

Dated: January 21, 2014

s/ Jonathan A. Strauss
Jonathan A. Strauss (#0279602)
Lorenz F. Fett (#196769)
Sonia Miller-Van Oort (#278087)
Kenn H. Fukuda (#0389301)
12 South Sixth Street, Suite 1242
Minneapolis, MN 55402
(612) 756-7100, Fax: 612-756-7101
jons@sapientialaw.com
larryf@sapientialaw.com
soniamv@sapientialaw.com
kennf@sapientialaw.com

ATTORNEY FOR PLAINTIFF KIRSTEN KENNEDY