

APPEAL NO. 22-CV-760

**DISTRICT OF COLUMBIA
COURT OF APPEALS**

ALEXA MOORE, ET AL.

Plaintiffs, Appellants

v.

DISTRICT OF COLUMBIA, ET AL.

Defendants, Appellees

**Appeal from the Superior Court for the
District of Columbia, Civil Division
Case No. 2021 CA 003834 B
(The Honorable Heidi M. Pasichow, Judge)**

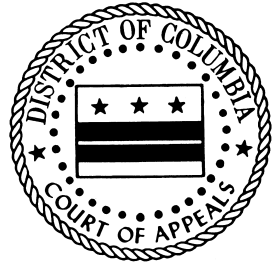
BRIEF OF APPELLANT ALEXA MOORE

*Arnold J. Abraham, Esq. (DC Bar No. 90003838)
CyberLaw, LLC, 220 N. Liberty Street, Baltimore, MD 21201
Phone: 443-906-3495

Eric J. Menhart, Esq. (DC Bar No. 975896)
Lexero Law, 512 C St NE, Washington, DC 20002
Phone: 855-453-9376

* Counsel expected to argue.

Attorneys for Appellants



Clerk of the Court
Received 01/02/2023 06:59 PM
Resubmitted 01/03/2023 10:30 AM
Resubmitted 01/03/2023 11:33 AM
Resubmitted 01/03/2023 02:15 PM
Resubmitted 01/03/2023 03:23 PM
Resubmitted 01/03/2023 05:02 PM
Filed 01/03/2023 05:02 PM

INTERESTED PARTIES

Pursuant to Rule 28(a)(2) of the Rules of the D.C. Court of Appeals, the undersigned counsel of record for the Appellants files this Certificate of Counsel and Parties.

Plaintiff, Alexa Moore

Eric Menhart, Esq.
Lexero Law
512 C St. NE
Washington, DC 20002
Counsel for Appellant

Arnold J. Abraham
CyberLaw, LLC
220 N. Liberty Street
Baltimore MD 21201
Counsel for Appellant

Defendant, The Metropolitan Police Department
Defendant, The District of Columbia
Defendant, the Office of the Chief Technology Officer

Elizabeth A. Scully, Esq.
Richard P. Sobiecky, Esq.
Pamela A. Disney, Esq.
c/o Baker & Hostetler LLP
Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5304
Counsel for Defendants

TABLE OF CONTENTS

INTERESTED PARTIES	2
TABLE OF AUTHORITIES	5
JURISDICTION	10
STATEMENT OF THE ISSUES.....	11
STATEMENT OF THE CASE	11
STATEMENT OF RELEVANT FACTS	14
STANDARD OF REVIEW	15
ARGUMENT.....	16
I. THE TRIAL COURT ERRED AS A MATTER OF LAW IN NOT APPLYING THE STANDARD OF REVIEW UNDER RULE 12(B)(6) WHICH REQUIRED INTERPRETATION OF FACTS IN THE LIGHT MOST FAVORABLE TO PLAINTIFF.	16
A. The Trial Court Did Not Take All of the Factual Allegations	16
in the Complaint as True	16
B. The Trial Court Erred When it Evaluated “Cyber Security” as a Single Overarching Discretionary Function Instead of Each of the Discrete Ministerial Sub-Tasks Described in the Complaint.....	18
C. The Proper Method of Evaluation for Whether a Task is Discretionary Versus Ministerial Requires Evaluation of the Facts of the Case Based on the Stage of the Proceedings.	21
D. The District Should Bear the Burden of Proof to Support its Claim of the Affirmative Defense of Sovereign Immunity, and It Was Not Required to Do So	25
II. THE TRIAL COURT ERRED AS A MATTER OF LAW WHEN IT RULED THE CLAIMS AGAINST THE DISTRICT OF COLUMBIA WERE BARRED UNDER THE SOVEREIGN IMMUNITY DOCTRINE.	26
A. Sovereign Immunity Does Not Apply to Ministerial Functions in the Complaint	26
B. The Trial Court Did Not Distinguish Between Ministerial and Discretionary Acts Alleged in the Pleadings	28
C. Statutory Law Governing the Applicable Functions Precludes Sovereign Immunity for Cybersecurity	39

D. The Court’s Cited Cases are Inapposite to its Ruling	42
CONCLUSION	43
STATEMENT AS TO TYPEFACE.....	45

TABLE OF AUTHORITIES

Cases

<i>Aguehoude v. District of Columbia</i> 666 A.2d 443 (D.C. 1995)	16,19, 21, 22, 23, 27, 40, 42
<i>Ashcroft v. Iqbal</i> 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009)	16
<i>Bell Atl. Corp. v. Twombly</i> 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)	17
<i>Berkovitz v. United States</i> 486 U.S. 531, 108 S. Ct. 1954 (1988)	39, 41
<i>Biscoe v. Arlington County</i> 738 F.2d 1352 (D.C. Cir. 1984)	35
<i>Bivens v. Six Unknown Named Agents of Fed. Bur. of Narc.</i> 456 F.2d 1339 (2d Cir. 1972)	18
<i>Carter v. Carlson</i> 447 F.2d 358, (D.C. Cir. 1971), rev'd in part on other grounds, 409 U.S. 418, 93 S. Ct. 602, 34 L.Ed.2d 613 (1973)	18, 35
<i>Casco Marina Dev., L.L.C. v. D.C. Redevelopment Land Agency</i> 834 A.2d 77 (D.C. 2003)	39
<i>Chandler v. District of Columbia</i> 404 A.2d 964 (D.C.1979)	29
<i>Cherry v. Dist. of Columbia</i> 330 F. Supp. 3d 216 (D DC 2018)	32
<i>Clampitt v. Am. Univ.</i> 957 A.2d 23, 29 (D.C. 2008)	15

<i>Cope v. Scott</i> 45 F.3d 445 (D.C. Cir. 1995)	27, 40
<i>D.C. Hous. Auth. v. Pinkney</i> 970 A.2d 854 (D.C. 2009)	29, 37
<i>Daigle v. Shell Oil Co.</i> 972 F.2d 1527 (10th Cir. 1992)	16
<i>District of Columbia v. North Wash. Neighbors, Inc.</i> 367 A.2d 143 (App. D.C. 1976)	16
<i>Elgin v. District of Columbia</i> 337 F.2d 152 (1964)	37
<i>Elliott v. District of Columbia</i> 160 F.2d 386 (1947)	38
<i>Florian v. Johnson</i> 2014 WL 5460815 (NJ Super App Div 2 Oct. 29, 2014)	34
<i>Fraser v. Gottfried</i> 636 A.2d 430 (D.C. 1994)	15
<i>ITSI TV Productions, Inc. v. Agricultural Ass'n.</i> 3 F.3d 1289 (9th Cir. 1993)	25
<i>J.C. v. District of Columbia</i> 199 A.3d 192 (D.C. 2018)	19, 24
<i>Johnston v. District of Columbia</i> 118 U.S. 19 (1886)	13, 21
<i>Lopez v. Southern California Rapid Transit</i> 40 Cal.3d 780, 221 Cal. Rptr. 840, 710 P.2d 907 (1985)	28
<i>Matthews v. Automated Bus. Sys. Serv.</i> 558 A.2d 1175 (D.C. 1989)	22

<i>McBryde v. Amoco Oil Co.</i> 404 A.2d 200 (D.C. 1979)	17
<i>McCummings v. Hurley Medical Center</i> 433 Mich. 404, 446 N.W.2d 114 (1989) (per curiam)	25
<i>McKethean v. WMATA</i> 588 A.2d 708, 715 (D.C. 1991)	23, 27
<i>Nealon v. District of Columbia</i> 669 A.2d 685 (D.C. 1995)	12, 26
<i>Owen v. City of Independence</i> 445 U.S. 622, 63 L. Ed. 2d 673, 100 S. Ct. 1398 (1980)	29
<i>Pelham v. United States</i> 661 F Supp. 1063 (D NJ 1987).	34
<i>Powell v. District of Columbia</i> 602 A.2d 1123 (D.C. 1992)	26
<i>Prescott v. United States</i> 973 F.2d 696 (9th Cir. 1992)	25
<i>Rustin v. District of Columbia</i> 491 A.2d 496 (D.C.), cert. denied, 474 U.S. 946, 106 S. Ct. 343, 88 L. Ed. 2d 290 (1985)	29
<i>Selma, R D.R. Co. v. United States</i> 139 U.S. 560, 11 S.Ct. 638, 35 L.Ed. 266 (1891).	25
<i>Sherbutte v. Marine City</i> 374 Mich. 48, 130 N.W. 2d 920 (1964)	18
<i>Stewart v. Nat'l Educ. Ass'n</i> 471 F.3d 169 (D.C. Cir. 2006)	17
<i>Thomas v. Johnson</i> 295 F. Supp. 1025 (D.D.C. 1968)	32

<i>Thompson v. District of Columbia</i> 570 A.2d 277 (DC 1990), vacated in part on other grounds, 593 A. 2nd 621 (DC 1991)	29
<i>United States v. Ross</i> 259 F. Supp. 388 (1966)	41
<i>United States v. Varig Airlines</i> 467 U.S. 797, 104 S.Ct. 2755, 81 L.Ed.2d 660 (1984)	27
<i>Urow v. District of Columbia</i> 316 F.2d 351 (D.C. Cir.) (per curiam), cert denied, 375 U.S. 826 (1963).	13, 21
<i>Usovan v. Republic of Turk.</i> 6 F.4th 31 (D.C. Cir. 2021)	27
<i>Wade v. District of Columbia</i> 310 A.2d 857 (D.C. 1973)	18
<i>Wagshal v. District of Columbia</i> 216 A.2d 172 (D.C. 1966)	43
<i>Walen v. United States</i> (D. D.C. 2019)	13, 20, 33
<i>Wash. Metro. Area Transit Auth. v. Nash-Flegler</i> 272 A.3d 1171 (D.C. 2022)	19, 28
<i>WMATA v. O'Neill</i> 633 A.2d 834 (D.C. 1993)	28
Statutes	
D.C. Code § 5-113.01(a)(3)	41
D.C. Code § 5-113.07	41

Treatises

18 E. MCQUILLIN, MUNICIPAL CORPORATIONS	
§ 53.22.10, at 274 (3d ed. 1984)20	29

JURISDICTION

Pursuant to Rule 28(a)(5) of the Rules of the D.C. Court of Appeals, counsel of record for the Appellant hereby assert that “the appeal is from a final order or judgment that disposes of all parties’ claims.”

STATEMENT OF THE ISSUES

- I. Whether the Trial Court Erred as a Matter of Law in Not Applying the Standard of Review for Dismissal under Rule 12(b)(6) which Required Interpretation of Facts in the Light Most Favorable to Plaintiff.
- II. Whether the Trial Court Erred as a Matter of Law When it Ruled the Claims Against the District of Columbia Were Barred Under the Sovereign Immunity Doctrine.

STATEMENT OF THE CASE

On October 21, 2021, the civil action was filed in the Superior Court for the District of Columbia by Plaintiff/Appellant Alexa Moore on behalf of herself and others similarly situated against *inter alia* the District of Columbia (“the District”) and its vendor contractors (“Contractor Defendants”) arising from a data breach in the computer system of the District causing the personal information of thousands of police officers and other employees of the District to be purloined. (App.-1). Under the Amended Complaint (“Am. Compl.”), Ms. Moore asserted claims against the District for Negligence (Count I) and Breach of Confidentiality (Count II). (App.- 2).

In response to the Amended Complaint, the District filed a motion to dismiss for failure to state a claim, arguing *inter alia*, that the claims of Ms. Moore and the putative class were barred by the doctrine of sovereign immunity. (App.-3).

On March 2, 2022, the lower court granted the District’s Motion to Dismiss (“Dismissal Order”). (App.-4). The Court determined that the claims against the District were barred by sovereign immunity. (App.-4; p. 8). Defendants Metropolitan Police Department and the Office of the Chief Technology Officer were dismissed because they were deemed not *sui juris* and therefore could not be sued in their own names. *Id.*

On June 17, 2022, the trial Court denied Plaintiff’s Motion for Rehearing and/or Reconsideration of its dismissal of the District (“Order Denying Rehearing”). (App.- 6). In its ruling the Court restated its finding as follows:

The doctrine of sovereign immunity acts as a bar to suing the District of Columbia for its discretionary functions. Nealon v. District of Columbia, 669 A.2d 685, 690 (D.C. 1995). Sovereign immunity applies to acts that are discretionary rather than ministerial, those that involve the formulation of policy and require personal deliberation, decision, and judgment. Id. In contrast, ministerial acts require little or no judgment and generally constitute mere obedience to orders of performance of a duty in which the municipal employee has little or no choice. Id. The Court found that Plaintiff’s claims implicate the District’s discretion concerning which protective measures to employ to protect data—precisely the type of discretion that is protected under the doctrine of sovereign immunity.

(Order Denying Rehearing- p. 5-6; App- 6: p. 5-6)

With ten short lines of text, the trial court’s ruling explained that the claims were barred as to the District under the sovereign immunity doctrine. In doing so, the Superior Court ignored the content of the complaint and instead made numerous assumptions in favor of the Defendants.

With this ruling, the Superior Court cast a wide blanket of immunity over all the District’s cybersecurity and privacy functions without evaluating whether actual components of the allegations would qualify as ministerial vice discretionary in nature. Such an approach does not comport with the law in general or specific precedent in this area.¹

The lower Court did not make any comment or ruling on the question of whether Plaintiff’s Amended Complaint complied with Rule 8(a). The Court did not make any comments or rule on the question of whether the District had a duty to protect Plaintiff’s personal information. The Court did not rule on whether the breach of confidentiality claim was appropriately pled based on an existing confidential relationship. While the Court provided a citation on the question of a “special relationship” it offered no comments and made no ruling on whether Plaintiff’s claims were barred by the so-called “Public Duty Doctrine.”

Each of the Contractor Defendants were subsequently dismissed without prejudice by consent of the parties. The matter was considered finally adjudicated

¹ See, *Walen v. United States* (D. D.C. 2019) discussing over a century of case law dealing with evaluating discrete sub-parts of common municipal functions to determine whether or not they were ministerial or discretionary functions, including the “obligation to keep streets in a safe condition after being put on notice of a defect” *Urow v. District of Columbia*, 316 F.2d 351 (D.C. Cir.) (*per curiam*), cert denied, 375 U.S. 826 (1963), at 352; and “decisions about the planning and design of its sewer system were discretionary but “for any negligence in . . . keeping [the sewer] in repair, . . . the municipality . . . may be sued.” *Johnston v. District of Columbia*, 118 U.S. 19 (1886),

on September 9, 2022. (App.- 7). This timely appeal addresses the dismissal of the claims against the District.

STATEMENT OF RELEVANT FACTS

The instant action involves claims arising from a data breach in the computer system supporting the Metropolitan Police Department within the District. The breach involved the theft and exposure of highly classified personal information of thousands of police officers and other employees of the District.

The Amended Complaint made numerous allegations about the District's acts, or lack thereof, within its cyber security and privacy protection posture that harmed the Plaintiff. These included some functions that could be described as discretionary and some that were clearly ministerial functions.

The Amended Complaint made numerous allegations characterizing the District's duty to perform cyber security and privacy functions. (Am. Compl- ¶¶183-202). Some of these duties were derived from statutory requirements and others based on industry standards. In both aspects, the range of its ability to exercise discretionary powers would therefore have been reasonably constrained by these existing guidelines.

Appellant does not believe it is necessary to recount the allegations of the Amended Complaint with respect to the many factual allegations of ministerial misfeasance. Suffice to say, the gist of the lawsuit is germane to all other lawsuits

asserting data breach liability: that the party entrusted with sensitive information failed to safeguard the data to the injury of others.

STANDARD OF REVIEW

When an appeal entails review of a motion to dismiss under Rule 12 (b)(6), the complaint is to be construed “in the light most favorable to appellant, accepting its allegations as true.” *Fraser v. Gottfried*, 636 A.2d 430 (D.C. 1994) (citations omitted). Moreover, because a motion to dismiss a complaint under Rule 12 (b)(6) presents questions of law, the standard of review for dismissal for failure to state a claim is *de novo*. *Id.* Because District of Columbia rules “reject the approach that pleading is a game of skill in which one misstep . . . may be decisive to the outcome’ and ‘manifest a preference for resolution of disputes on the merits, not on technicalities of pleading,’ pleadings are to be construed ‘as to do substantial justice.’” *Clampitt v. Am. Univ.*, 957 A.2d 23, 29 (D.C. 2008) (*quoting Carter-Obayuwana v. Howard Univ.*, 764 A.2d 779, 787 (D.C. 2001)).

Plaintiff’s Complaint meets the necessary standards to preclude dismissal of her claims. Accordingly, this Court of Appeals must reverse the Superior Court’s grant of Appellees’ Motions to Dismiss unless the Appellant has failed to adequately plead facts that would disclose a legally sufficient cause of action, drawing all inferences from such facts in favor of Appellant.

The essential element of the Superior Court’s ruling was that the allegations involved a discretionary function. Whether a function is discretionary or ministerial is a question going to the subject matter jurisdiction of the trial court. *District of Columbia v. North Wash. Neighbors, Inc.*, 367 A.2d 143, 148 n. 7 (App. D.C. 1976). It is a determination to be made by the trial judge, not the jury. *Aguehounde v. District of Columbia*, 666 A.2d 443, 447 (D.C. 1995). Therefore, the standard for review is a *de novo* review of the trial court's determination of whether or not the action was discretionary. See e.g., *id.*; *Daigle v. Shell Oil Co.*, 972 F.2d 1527, 1537-1539 (10th Cir. 1992).

ARGUMENT

I. THE TRIAL COURT ERRED AS A MATTER OF LAW IN NOT APPLYING THE STANDARD OF REVIEW UNDER RULE 12(B)(6) WHICH REQUIRED INTERPRETATION OF FACTS IN THE LIGHT MOST FAVORABLE TO PLAINTIFF.

A. The Trial Court Did Not Take All of the Factual Allegations in the Complaint as True

Plaintiffs are generally provided a generous standard to avoid dismissal of pleadings. But in this case, the Superior Court overlooked the well-pled allegations supporting a theory of liability based on ministerial acts outside the scope of sovereign immunity.

In analyzing a motion to dismiss under Rule 12(b)(6), a court “must take all of the factual allegations in the complaint as true.” *Ashcroft v. Iqbal*, 556 U.S. 662,

678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (*quoting Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). *Id.* It also must “constru[e] the complaint liberally in the plaintiff’s favor with the benefit of all reasonable inferences derived from the facts alleged.” *Stewart v. Nat’l Educ. Ass’n*, 471 F.3d 169, 173 (D.C. Cir. 2006). Further, a motion to dismiss for failure to state a claim should be granted only if “it appears beyond a doubt that [the plaintiff] can prove no set of facts in support of his claim which would entitle him to relief.” *Id.* (*citing McBryde v. Amoco Oil Co.*, 404 A.2d 200, 202 (D.C. 1979)).

In contrast to this requirement, the Court not only failed to find that “no set of facts” could support the claim, but also went even further by rejecting the specific facts as alleged and instead chose to adopt a different characterization of events that was propounded by the Defendant in support of their position.

The Amended Complaint contained more than seventy (70) detailed allegations in the “Negligence” portion alone that focused on distinct aspects of the cybersecurity and privacy functions for which the District was responsible. (Am. Compl- ¶¶183-202; App. 2). In order for the Court’s ruling to hold, each of these allegations must have been accepted as true. However, the Court ignored the contents of the pleadings, which not only alleged failures in the District’s choices regarding the implementation, but also in the execution of these functions. The Amended Complaint, which was necessarily broad given the absence of discovery,

included the contention that the District's failure was due to errors in both design and implementation. Because many of these allegations included ministerial tasks, it would not have been possible for the Court to have accepted them as pled. Therefore, the trial court decision must be reversed.

B. The Trial Court Erred When it Evaluated "Cyber Security" as a Single Overarching Discretionary Function Instead of Each of the Discrete Ministerial Sub-Tasks Described in the Complaint.

The Superior Court painted with too broad a brush in reaching its conclusion. If the complaint had alleged a single broad claim of "inadequacy of the District's cybersecurity posture" then perhaps the trial court's ruling could be explained. However, given the numerous specific tasks delineated in the complaint, it was an error to simply make a single evaluation of the overarching function of cybersecurity.

There is often a very different outcome when analyzing discrete subcomponents rather than overarching categories. Consider the contrast between "without question the operation of a police force is a governmental function" *Wade v. District of Columbia*, 310 A.2d 857, 860 (D.C. 1973) and "it settled that for immunity purposes the act of making an arrest is ministerial." *Bivens v. Six Unknown Named Agents of Fed. Bur. of Narc.*, 456 F.2d 1339 (2d Cir. 1972); *Carter v. Carlson, supra*; *Sherbutte v. Marine City*, 374 Mich. 48, 130 N.W. 2d 920 (1964)." *Wade v. District of Columbia*, 310 A.2d 857, 860 (D.C. 1973).

The evaluation as to whether a matter in dispute is discretionary or ministerial requires the proper level of detail. For example, in a case dealing with an accident at an intersection, the court did not make a ruling on “traffic safety” but instead evaluated the specific task which was described in the complaint - setting the timing of the signal intervals. *Aguehounde v. District of Columbia*, 666 A.2d 443, 448 (D.C. 1995).

To emphasize this requirement, the District of Columbia Court of Appeals made it clear that the proper evaluation could not be just the broad function of “child protective services” but that the nature of the specific alleged actions needed to be evaluated. *J.C. v. District of Columbia*, 199 A.3d 192 (D.C. 2018).

Finally, this jurisdiction’s most recent decision dealing with the question of “discretionary” versus “ministerial” discusses this concept extensively when evaluating the placement of a single warning cone rather than the broad categories of public transportation safety and the general principle of failure to warn. *Wash. Metro. Area Transit Auth. v. Nash-Flegler*, 272 A.3d 1171 (D.C. 2022).

The need for a complete and thorough evaluation of what may be discretionary versus ministerial is even more clear in the present case. While *Aguehounde*, *J.C.*, and *Nash-Flegler* each involved discrete incidents affecting individuals, this case includes a wide variety of alleged failures over an extended period of time. Such

errors occurred repeatedly and involved numerous shortfalls in dozens of specific ministerial subtasks that ended up impacting thousands of people.

The Amended Complaint made numerous allegations about the District's acts, or lack thereof, that must qualify as ministerial in nature in the absence of clear evidence they were discretionary (policy) decisions. But despite the existence of these allegations, the lower Court ruled that all aspects (and alleged failures) of the District's cyber security function were discretionary (as a matter of law) without any evaluation of what each of those steps were and what specific failures were alleged to have occurred. The function to develop, maintain, and execute cybersecurity and privacy protocols for the entire police department was clearly a significant undertaking for the District. There is no indication from its ruling that the Court made any inquiry into the nature of these specific allegations of negligence. Instead, it cast a wide blanket of immunity over all cybersecurity and privacy functions, in a manner akin to saying the broad functions of policing, public sanitation, or public transportation are fully protected without the need to refine these subjects further to determine what specific sub activity is actually the matter under contention. This is contrary to what the law requires. *See Walen v. United States* (D.D.C. 2019) (discussing over a century of case law dealing with evaluating discrete sub-parts of common municipal functions to determine whether or not they were ministerial or discretionary functions, including the "obligation to keep streets in a safe condition

after being put on notice of a defect”); *Urow v. District of Columbia*, 316 F.2d 351 (D.C. Cir.) (per curiam), *cert denied*, 375 U.S. 826 (1963), at 352; (decisions about the planning and design of its sewer system were discretionary but “for any negligence in . . . keeping [the sewer] in repair, . . . the municipality . . . may be sued.”); *see also Johnston v. District of Columbia*, 118 U.S. 19 (1886).

The NIST Cybersecurity Framework² breaks down cybersecurity into six different functions of Identify, Protect, Detect, Respond, and Recover. The NIST Cybersecurity Framework further provides over one hundred subcategories of tasks that all should be individually considered as part of an organizations’ cybersecurity posture. These NIST functions were described extensively through dozens of pages of allegations in the Complaint. It is clear the lower Court did not evaluate each of these functions and tasks when it concluded that the entire universe of cybersecurity could only be discretionary as a matter of law.

C. The Proper Method of Evaluation for Whether a Task is Discretionary Versus Ministerial Requires Evaluation of the Facts of the Case Based on the Stage of the Proceedings.

In *Aguehoude v. District of Columbia*, the Court found that within the overarching category of traffic safety, the specific task of setting the length of the clearance interval in crosswalks involved policy considerations and was

² <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

discretionary. *Aguehounde*, 666 A.2d at 445. However, it is important to recognize that before the trial court came to its final decision in that matter, two Superior Court judges had ruled at earlier stages of the litigation that the exact function under consideration was ministerial, rather than discretionary, in nature. *Id.* at 461. Those earlier rulings were made in response to motions for summary judgment and for directed verdict. But in the present case, the standard was at the stage where the bar would be at the absolute highest for the defendant and lowest for the plaintiff. To be sure, if after discovery, there were no facts that showed ministerial misconduct, the District would be entitled to summary disposition as in *Aguehounde*.

Further, in *Aguehounde* the Court recognized that when determining whether the act is discretionary, the trial court is not confined to considering only that evidence which was also heard by the jury; instead, the court may consider all evidence coming to its attention bearing on that issue. *Id.* at 447; *see also*, *Matthews v. Automated Bus. Sys. Serv.*, 558 A.2d 1175, 1179-80 (D.C. 1989) (“the court has broad discretion in determining how to proceed in finding such [jurisdictional] facts, including basing its decision on affidavits”). In stark contrast, in the instant case, the lower Court not only did not have the opportunity to consider the evidence heard by the jury (as there was none), it also did not have the benefit of reviewing any evidence **at all** since the matter had never been permitted to leave the initial pleading stage.

The required depth of analysis for the determination in this case was clearly lacking. In *Aguehoude*, when the Court found the timing of signal intervals involves balancing various economic, political, and social considerations it did so by recognizing a number of complex factors were involved:

considerations of safety not only for pedestrians but for travelers, and it involves a balancing of safety needs against the need to assure adequate traffic flow, which itself involves considerations of safety as well as commerce and convenience. Balancing these factors also requires the ascertainment of facts, such as numbers of vehicles and pedestrians, and ways in which drivers and pedestrians behave in the aggregate, which are peculiarly subject to study and expertise. Subjecting the decisions of traffic engineers to litigation and to second-guessing by jurors would deter effective government.

Aguehoude, 666 A.2d at 448.

While some aspects of cybersecurity may rise to the level of “balancing various economic, political and social considerations,” most functions are not. The failure to train and supervise employees to avoid opening a zip file containing a virus, or to avoid clicking a hyperlink to malware, involves no such consideration. There is “no second guessing” as every person and organization must be vigilant to guard against outside cyberattacks.³

The trial court must determine whether the act is a discretionary or ministerial function under the circumstances presented. *McKethean v. Wmata*, 588 A.2d 708 at

³ For an informative discussion of the basic cyber-security measures, see <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> and <https://consumer.ftc.gov/articles/protect-your-personal-information-data>

715 (D.C. 1991). In the present case there was no indication from the Court's ruling that there was any consideration of the circumstances presented. Therefore, the trial court erred, and at a minimum the case would need to be remanded for full and proper evaluation. However, it is not clear how the lower Court could possibly evaluate the evidence, considering discovery had not even been initiated, so the ruling should simply be reversed and the litigation allowed to continue its course.

In the case of *J.C. v. District of Columbia*, a suit was brought against the District after a report of child abuse resulted in the government's removal of minor children from their parents. The trial court concluded that all of the District's actions at issue were discretionary, rather than ministerial. Upon appeal, the case was remanded for the trial court to analyze the issue of sovereign immunity more carefully in light of the specific actions being challenged and in light of the specific evidence. Additionally, the trial court was instructed to address the extent to which each specific action alleged was or was not driven by a District policy. *J.C.*, 199 A.3d at 206. These same issues would have required more careful analysis to support the ruling the Court reached. However, given the stage of the proceedings that the current case was in, no such further analysis is required because the matter was to be decided in the light most favorable to the plaintiffs.

D. The District Should Bear the Burden of Proof to Support its Claim of the Affirmative Defense of Sovereign Immunity, and It Was Not Required to Do So.

“[I]t has been established as a general rule that the burden of proof lies on the person who wishes to support his case by a fact which lies peculiarly within his knowledge, or of which he is supposed to be cognizant.” *Selma, R D.R. Co. v. United States*, 139 U.S. 560, 568, 11 S.Ct. 638, 640, 35 L.Ed. 266 (1891) (citations omitted); *see also, ITSI TV Productions, Inc. v. Agricultural Ass'n.*, 3 F.3d 1289, 1292 (9th Cir. 1993). Applying this principle to a governmental claim of immunity, other States have found that the burden of demonstrating governmental immunity is on the defendant. *McCummings v. Hurley Medical Center*, 433 Mich. 404, 446 N.W.2d 114, 117 (1989) (per curiam); *Kolitch v. Lindedahl*, 100 N.J. 485, 497 A.2d 183, 189 (1985).

By analogy, the federal appellate courts have unanimously concluded that when the “discretionary function” exception to the Federal Tort Claims Act is invoked as a defense against a facially sufficient complaint the United States bears the burden of proving that the particular governmental action falls within the scope of that exception. *See Prescott v. United States*, 973 F.2d 696, 701-02 (9th Cir. 1992) (citing authorities). “If the government desires to rely upon any of [the] provisions [exempting it from liability for the exercise of a discretionary function], it has a right

to do so in defense of the action, providing such defense is aptly pleaded and proven.” *Stewart, supra* note 1, 199 F.2d at 520.

The District is the only party which had unrestricted access to all of the information relevant to its claim of immunity. What the District's employees did, why they did it, and what factors they considered, are facts readily known only to the District. Therefore, in cases such as the present matter, where there is not a preponderance of evidence to support sovereign immunity, the claim should, at the very minimum, survive a motion to dismiss.

II. THE TRIAL COURT ERRED AS A MATTER OF LAW WHEN IT RULED THE CLAIMS AGAINST THE DISTRICT OF COLUMBIA WERE BARRED UNDER THE SOVEREIGN IMMUNITY DOCTRINE.

The Court’s finding that the “doctrine of sovereign immunity” bars Plaintiff’s claims was an error because (a) applicable common law demonstrates the District’s negligence was based on failures in ministerial functions and (b) applicable statutory law precludes any finding of “discretionary acts” in the instant case.

A. Sovereign Immunity Does Not Apply to Ministerial Functions in the Complaint

“The doctrine of sovereign immunity acts as a bar to bringing suit against the District of Columbia for its discretionary functions.” *Nealon v. District of Columbia*, 669 A.2d 685, 690 (D.C. 1995) (citing *Powell v. District of Columbia*, 602 A.2d 1123, 1126 (D.C. 1992)). The question as to whether immunity is available under

the doctrine turns upon whether the act complained of was discretionary or ministerial. *Id.* (citing *Powell*, 602 A.2d at 1126).

The District is immune only if the act was committed in the exercise of discretionary functions. *Id.* (citing *Aguehoude v. District of Columbia*, 666 A.2d 443 (D.C. 1995)); *McKethean v. WMATA*, 588 A.2d 708, 715 (D.C. 1991). If the act is committed in the exercise of a ministerial function, the District is not immune. *Id.* (citing *Powell*, 602 A.2d at 1126; *McKethean*, 588 A.2d at 715).

Administrative decisions which require the government to balance competing considerations are considered discretionary acts. *McKethean*, 588 A.2d at 715. By barring suit for such actions, Congress “prevent[s] judicial ‘second-guessing’ of legislative and administrative decisions grounded in social, economic and political policy through the medium of an action in tort.” *United States v. Varig Airlines*, 467 U.S. 797, 814, 104 S.Ct. 2755, 2764, 81 L.Ed.2d 660 (1984).

The determination that a function qualifies as discretionary to the point that it triggers sovereign immunity is not to be taken lightly because “[N]early every government action is, at least to some extent, subject to ‘policy analysis,’” and a decision is not protected by sovereign immunity simply because it involves “the faintest hint of policy concerns.” *Cope v. Scott*, 45 F.3d 445, 448-49 (D.C. Cir. 1995); *Usovan v. Republic of Turk.*, 6 F.4th 31, 45 (D.C. Cir. 2021). The mere presence of choice does not trigger sovereign immunity and when there is no

evidence that a decision was in fact animated by policy concerns, at least, sovereign immunity will apply only if the “nature” of the decision itself is “fraught... with public policy considerations.” *Wash. Metro. Area Transit Auth. v. Nash-Flegler*, 272 A.3d 1171, 1181 (D.C. 2022) citing *Cope*, 45 F.3d at 450; *Usovan*, 6 F.4th at 47. Finally, “[t]he fact that in a particular case an [employee] might have alternative courses of action from which to choose, and this choice might involve a certain degree of judgment, does not elevate the [employee’s] decision to the level of ‘basic policy.’” *WMATA v. O’Neill*, 633 A.2d 834, 839 (D.C. 1993) (quoting *Lopez v. Southern California Rapid Transit*, 40 Cal.3d 780, 221 Cal. Rptr. 840, 849, 710 P.2d 907, 916 (1985)).

Many of the allegations in the Complaint are outside the bounds of what would qualify under the doctrine as described above, and therefore sovereign immunity does not apply in this case.

B. The Trial Court Did Not Distinguish Between Ministerial and Discretionary Acts Alleged in the Pleadings

In the Dismissal Order, the Court cited decisions that stood for the proposition that “design” functions were discretionary and therefore exempted by the Sovereign Immunity Doctrine. In contrast to other cases where it has been recognized that “[c]haracterizing an act as discretionary or ministerial is not always an easy task,” the Superior Court here provided only a conclusory statement on the question of ministerial versus discretionary functions rather than applying existing methods to

testing the categorization. *McKethan*, 588 A.2d at 715. Additionally, the Superior Court overlooked that the Amended Complaint provided a litany of allegations related to the District’s ministerial acts that involved failures of “performance of duties” as opposed to policy decisions by the District.

Discretionary acts have also been defined as acts that require “personal deliberation, decision and judgment.” *Id.* (citing 18 E. MCQUILLIN, MUNICIPAL CORPORATIONS § 53.22.10, at 274 (3d ed. 1984)). Such functions generally have “a broad public effect and call for ‘a delicate balancing of competing considerations.’” *Id.* (citing *McKethan*, 588 A.2d at 715 (quoting *Owen v. City of Independence*, 445 U.S. 622, 648, 63 L. Ed. 2d 673, 100 S. Ct. 1398 (1980))). “Generally, discretionary acts involve the formulation of policy, while ministerial acts involve the execution of policy.” *D.C. Hous. Auth. v. Pinkney*, 970 A.2d 854, 860 (D.C. 2009) (citing *Nealon*, 669 A.2d at 690).

The Court’s ruling that *all aspects* of the District’s computer security were discretionary functions is almost impossible to be correct. In many instances it is a simple matter to distinguish between discretionary and ministerial acts, but in many cases, like this one, the question is a fact-specific determination. As stated by this Court in *Thompson v. District of Columbia*, 570 A.2nd 277 (DC 1990), *vacated in part on other grounds*, 593 A. 2nd 621 (DC 1991):

We have said, speaking generally, that discretionary functions concern “formulation” of policy, whereas ministerial functions concern

“execution” of policy. *Rustin v. District of Columbia*, 491 A.2d 496, 500 (D.C.), cert. denied, 474 U.S. 946, 106 S. Ct. 343, 88 L. Ed. 2d 290 (1985); see *Chandler v. District of Columbia*, 404 A.2d 964, 965-66 (D.C.1979). More specifically, we have said that this distinction turns on whether imposition of liability would more likely encourage or inhibit conscientious, effective performance of the particular governmental function at issue. See *Rustin*, 491 A.2d at 500; *Chandler*, 404 A.2d at 966. One way of testing this distinction is to ask whether, in evaluating particular governmental functions, there is any reason “to believe a jury could render a sounder decision than those officials chosen, qualified, and prepared to make them.” *Id.*, quoted in *Rustin*, 491 A.2d at 500.

We are aware that the discretionary-ministerial distinction can be elusive, for “virtually all official acts involve some modicum of choice.” *Id.* at 298. Accordingly, absent legislative guidelines, we must select our own policy factors to determine whether the governmental action at issue allows significant enough application of choice to justify official immunity, in order to assure “fearless, vigorous, and effective” decision-making. *Barr*, 360 U.S. at 571, 79 S. Ct. at 1339. Persuaded by Professor Keeton’s analysis, we believe the applicable policy factors should be “[1] the nature of the plaintiff’s injury, [2] the availability of alternative remedies, [3] the ability of the courts to judge fault without unduly invading the executive’s function, and [4] the importance of protecting particular kinds of official acts.” *PROSSER & KEETON* § 132, at 1062. See also *RESTATEMENT (SECOND) OF TORTS* § 895D, comment f.

Id. at 297.

Even assuming the District’s position that many of the allegations in the complaint fell within the realm of policy judgment, this would not relieve them from liability for the well-pled failures that were purely ministerial in nature. The Amended Complaint alleged a wide variety of acts or omissions that would clearly qualify as ministerial as well as some allegations that would require further investigation to properly categorize.

The analysis cannot be completed without fact finding as to the ministerial and discretionary acts to realize answers as to the causation of the harm. For example, did the District make an intentional policy decision to not provide adequate cybersecurity? Was the failure to implement the network security measures recommended by the FBI, Homeland Security, and Microsoft, a discretionary policy decision? Or was their failure in carrying out the procedures due to a careless attendee flipping the wrong switch? Were their firewalls deliberately configured according to their chosen specifications and yet still inadequate to the task, or was there some lack of attention to detail that left a back-door open despite clear guidance that would have prevented the attack if the instructions were implemented as directed?

It was impossible to answer such questions at the stage of the proceedings the case was in when the Court made its ruling. The pleadings should not have been dismissed based on a misplaced conclusion that the damages to the Plaintiff were due to discretionary acts when the pleadings clearly alleged a combination of both discretionary and ministerial failures.

A review of case law shows many subsets of functions associated with a cyber security program have previously been held as ministerial and not discretionary. Such functions include training, maintaining, and updating the infrastructure, proper use of software, adhering to safety and security protocols.

Training: Conducting training and instructing are ministerial acts, not discretionary ones and are therefore not subject to the exemption of Sovereign Immunity. *Cherry v Dist of Columbia*, 330 F. Supp. 3d 216 (D DC 2018). In *Cherry*, the use of force by law enforcement officers led to the death of the plaintiff whose estate filed suit for violation of Fourth Amendment rights and alleged that the District “intentionally and with deliberate indifference” and “failed to train its officers in the proper application of force.” *Id.* The *Cherry* court concluded that although the decision regarding the appropriate level of training can be considered discretionary, “Once the decisions have been made to have a police department, to organize it in a particular way, and to hire a specific individual to be a member of that department, the acts of training, instructing, supervising, and controlling the individual officer are merely “ministerial.” A municipality can be held liable for negligently performing them. *Id.*; see also *Thomas v. Johnson*, 295 F. Supp. 1025 (D.D.C. 1968) at 1030–31. (“the tasks of supervising and instructing officers are ministerial, not discretionary acts” because “they do not involve the kind of policy-formulating, judgment-making processes encompassed by the term ‘discretionary.’”)

A cyber security program must train all relevant personnel to protect sensitive data and identify and report potential cyber security threats. Construing the situation at hand in the light most favorable to the Plaintiff, it is a credible belief that the

Defendant fell short in the ministerial tasks of training and instructing aspects of its cybersecurity program.

Failure to Maintain or Update Security Software. Failure to install timely updates to cyber security software is a ministerial act not subject to the protection of Sovereign Immunity. The *McKethean* decision stands for the proposition that decisions regarding design are discretionary, as opposed to maintenance operations which are ministerial. The *McKethean* court distinguished “allowing the bus stop in question to deteriorate” as separate from the discretionary functions of protected by Sovereign Immunity. Allowing a physical structure to deteriorate and allowing a cyber structure such as a firewall to deteriorate are equal in this regard as ministerial in nature.

Once the District made the design decisions regarding its cyber security posture, the maintenance of that security posture must be viewed in the same manner as the maintenance of the safety posture of its roadways. *See Walen v. United States* (D. D.C. 2019) (noting that the decision whether or not to put up a traffic sign in a particular location may be discretionary, but once it is in place the defendant “had a duty to maintain it properly in order to maintain safety” and “keeping the roadway and its physical appurtenances in good condition, according to their original design” fits into the definition of ministerial activity). Just as they would have been responsible for repair of a pothole after being “put on notice,” the District was liable

for failure to adequately secure its computer networks after being put on notice of its vulnerability.

Cyber safety/security and roadway safety/security are analogous. Both are areas that connect people to vital goods and services and on which travelers can be subject to devastating harm if safety programs are not maintained according to original design. Therefore, once a cyber security system was put in place, the District had a duty to maintain it. Failure to do so according to its original design was a failure in ministerial functions.

The failure can be found in several discrete parts:

1. Proper use of Software. Even beyond the need to keep it up to date with patches, the simple act of using software in conduct of automated processes has been considered ministerial. *See Florian v Johnson*, 2014 WL 5460815 (NJ Super App Div 2 Oct. 29, 2014) (holding use of software to designate students to particular stops and generate bus passes was ministerial). In this case, it is a near certainty that the District used software programs in execution of its cyber security functions that were alleged to be negligent, such as the programs that detect viruses or monitor intrusion.

2. Implementation and Monitoring of Safety and Security Protocols. Other jurisdictions have found implementation of safety regulations to be a ministerial and not discretionary function. *Pelham v United States*, 661 F Supp. 1063

(D.N.J. 1987). In *Pelham*, a project engineer's inspection and challenge to a potential violation of safety program rules in a previously designed safety program was considered ministerial and not discretionary. *Id.* at 1072-73. Similarly, cyber security programs have security protocols that apply to contractors, remote workers and general personnel and these regulations must be monitored in order to maintain the effectiveness of the program. The actions taken to ensure adherence to these protocols (or omissions of such actions) are ministerial.

3. Day-to-Day Operations. At the broadest level, the overall day-to-day operation of the District's computer networks represents the essential "ministerial" tasks of the information age. Plowing the field or manning the assembly line has been replaced with stringing cable and typing code on the keyboard. "[F]rom the very nature of these activities, it is clear that they do not involve the kind of policy formulating, judgment-making processes encompassed by the term discretionary." *Biscoe v. Arlington County*, 738 F.2d 1352, 1362 (D.C. Cir. 1984) *quoting Thomas*, 295 F. Supp. at 1031. Day-to-day operational matters like these are ministerial while planning and policy are discretionary. Further, management of the information security organization itself, through the Office of the Chief Technology Officer, falls in this mixed category. It has been recognized that supervising and controlling personnel involves a variety of both ministerial and discretionary functions. *Carter*

v. Carlson, 447 F.2d 358, 363–64 (D.C. Cir. 1971), *rev'd in part on other grounds*, 409 U.S. 418, 93 S. Ct. 602, 34 L.Ed.2d 613 (1973)).

As noted above, Plaintiff's claims directly relate to failures of "performance of duties" as opposed to only specific policy⁴ decision undertaken by the District. The Amended Complaint made a litany of allegations about the District's acts, or lack thereof, that harmed the Plaintiff and the putative class:

- "has not acted reasonably to protect the stolen identities of its officers." *See* Amended Complaint at ¶ 126.
- "did not reasonably protect the Plaintiff and putative Class Members' data while in its custody and control." *Id.* at ¶ 127.
- "marked certain Plaintiff and Class Member information in their possession as 'Confidential.'" *Id.* at ¶ 283
- "collected, stored, and maintained Plaintiff's and Class Members' Personal Information." *Id.* at ¶ 284.
- "failing to abide by their own privacy and internet policies." *Id.* at ¶ 290.
- "failure to prevent and avoid the Data Breach from occurring," *Id.* at ¶ 291.
- "After the breach occurred, Plaintiff heard from other MPD members that the breach occurred through a remote worker in the 'Time and Attendance Unit.' This unit was responsible for inputting time records in the 'TACIS System.'" *Id.* at ¶ 178.

⁴ As discussed in detail below, there was no opportunity, of any kind, to create "policy" in the instant case, because of the existence of statutory requirements related to the maintenance of the data in question.

- “As a direct and proximate cause of Government Defendants’ actions and/or omissions, Plaintiff and Class Members have suffered damages.” *Id.* at ¶ 292.
- “did not perform on its promises to safeguard Plaintiff’s and Class members’ sensitive personal information and to maintain a secure network.” *Id.* at ¶ 299.

Plaintiff’s allegations include “actions and/or omissions” undertaken within the data storage environment that was already created and operating when the errors arose rather than only broad policy decisions.

Prior cases are instructive. In one matter, “a minor and a full-time student at a public school owned and operated by the District of Columbia, was engaged in a required recreation program on the school playground.” *Elgin v. District of Columbia*, 337 F.2d 152, 153 (1964). The student fell in a depressed area of the play area. The Complaint generally alleged (a) “negligence in failing either to provide, or to maintain properly, an adequate railing or other safeguard,” and (b) exposing the student “to this dangerous condition through mandatory participation in activities likely to result in injury.” *Id.* In holding that the District was not immune from liability, the Court held that “the school playground was not only a public area which [the child] was privileged to traverse but one in which he was affirmatively required to be at the time of his injury.” *Id.* at 157.

Similarly, this Court held that “‘maintenance of elevators in a residence facility over which [the governmental entity] has responsibility’” is not a discretionary function that qualifies for sovereign immunity. *D.C. Hous. Auth. v. Pinkney*, 970 A.2d 854, 863 (D.C. 2009). The District was negligent in maintaining elevators in a facility over which the District had complete administrative control, a public residence facility.

In another matter, the Court held that “as the [trial] court recognized it has long been settled that the District of Columbia is under a duty to use reasonable care to keep its streets safe.” *Elliott v. District of Columbia*, 160 F.2d 386, 387 (1947). The Court went on to hold that, “whether it is or is not negligent to maintain a sidewalk . . . depends, like other questions of negligence, on the circumstances of the particular case.” *Id.* The Court went on to decide that “other questions of negligence” depended “on the circumstances of the particular case.” *Id.*

In each of the above cases, the Plaintiff was injured by the District’s negligence in maintaining assets that were entirely within the District’s control. In *Elgin*, the school child was injured on a playground entirely under the District’s control, and the child was required to be recreating on the playground. In *Elliott*, the injury was caused by a sidewalk maintained by the District. Here, Plaintiff and her fellow employees were injured by the District’s failure to maintain adequate security on computer equipment completely owned and operated by the District. Also, like

the obligatory actions seen in *Elgin*, the Plaintiff in this matter was required to have her personal data stored by the District.

The teachings of this Court show the particular circumstances of the instant case must be litigated on the merits. Dismissal is accordingly not appropriate.

C. Statutory Law Governing the Applicable Functions Precludes Sovereign Immunity for Cybersecurity

The United States Supreme Court has expressly held that “the discretionary function exception will not apply when a federal statute, regulation, or policy specifically prescribes a course of action for an employee to follow. In this event, the employee has no rightful option but to adhere to the directive.” *Berkovitz v. United States*, 486 U.S. 531, 536, 108 S. Ct. 1954, 1958-59 (1988). “The discretionary function exception applies only to conduct that involves the permissible exercise of policy judgment.” *Id.* at 1960.

Relying on this holding, the D.C. Court of Appeals has referred to “comparable municipal regulation[s]” in finding that no immunity exists when a statutory obligation exists. *Casco Marina Dev., L.L.C. v. D.C. Redevelopment Land Agency*, 834 A.2d 77, 82 (D.C. 2003) (reversing a finding of immunity for the D.C. Redevelopment Land Agency).

Therefore, even if the District met the burden of showing ALL the allegations involved acts that were discretionary in nature, sovereign immunity would still not apply here. As stated by this Court:

We often contrast discretionary functions with “ministerial” acts in which a “statute, regulation, or policy specifically prescribes a course of action” so that there is “no rightful option but to adhere to the directive.” *Barksdale-Showell*, 965 A.2d at 21 (quoting *United States v. Gaubert*, 499 U.S. 315, 322-23, 111 S. Ct. 1267, 113 L.Ed.2d 335 (1991)). But importantly, not every non-ministerial act is a discretionary act protected by sovereign immunity. “Only discretionary actions ‘grounded in social, economic, and political policy’” are protected. *Usayan v. Republic of Turkey*, 6 F.4th 31, 45 (D.C. Cir. 2021) (quoting *Gaubert*, 499 U.S. at 323, 111 S.Ct. 1267)).

Wash. Metro Area Transit Auth. v. Nash-Flegler, 272 A.3d 1171, 1181 n.3 (D.C. 2022).

In the instant matter, “specific directive exists which removes the otherwise unfettered discretion of the government employee” therefore “opening the government to suit if not performed correctly.” *Aguehounde*, 666 A.2d at 448. The Complaint speaks to many of the instruments of controlling guidance that dictate various constraints for the District’s cyber security posture. *See Cope v. Scott*, 45 F.3d 445, 448 (DC 1995) (“If a specific directive exists . . . [t]he only issue is whether the employee followed the directive”).

While detailing the full suite of such directives and controlling guidance would require completion of discovery, at least some of those can be cited here. For example, statutes expressly *mandate* that the digital records in question in this case be maintained. One D.C. statute, entitled “§ 5-113.01. Records — Required” provides that:

(a) The Mayor of the District of Columbia shall cause the Metropolitan Police force to keep the following records:

(3) A personnel record of each member of the Metropolitan Police force, which shall contain his name and residence; the date and place of his birth; his marital status; the date he became a citizen, if foreign born; his age; his former occupation; and the dates of his appointment and separation from office, together with the cause of the latter;

See D.C. Code § 5-113.01(a)(3).

Moreover, another statute, entitled “§ 5-113.07. Preservation and destruction of records” provides that:

All records of the Metropolitan Police Department shall be preserved, except that the Mayor, upon recommendation of the Chief of the Metropolitan Police Department and only pursuant to part B of this subchapter, may cause records which the Metropolitan Police Department considers to be obsolete or of no further value to be destroyed.

See D.C. Code § 5-113.07.

While the mandates of the statutes are clear, one case expressly notes that these statutes were specifically designed to be “matters of law and *not* of administrative discretion.” *United States v. Ross*, 259 F. Supp. 388, 390 (1966) (emphasis added). The Supreme Court has ruled that “the discretionary function exception will not apply” when an employee had “no rightful option but to adhere to the directive.” *Berkovitz v. United States*, 486 U.S. 536 (1988). The instant case falls comfortably into a category where “discretion” may not be legally concluded given the noted statutory requirements. Given that there is no possibility of a finding of a discretionary act, sovereign immunity is not available to the District in this case.

This case is distinguishable from others where no statutes or regulations were cited which would have limited the discretion of the District (such as in the decision to relocate bus stops). *See, Berkovitz*, U.S. at 536, 542-548. In *Aguehounde*, the Court at least considered the contention that specific mandates existed to limit discretion and transform the function into a ministerial one before ultimately concluding that was not a determinative factor. *Aguehounde*, 666 A.2d at 452. (“Our review of the evidence confirms the trial judge’s findings that there was no policy or specific directive mandating that District engineers follow the formula contained in the chart.”) Here, the Superior Court apparently gave no such consideration to the plainly stated allegations that, at least in some areas, numerous existing mandates equated to dispositive limitations on discretion.

D. The Court’s Cited Cases are Inapposite to its Ruling

Three of the cases cited in support of the Superior Court’s decision were not accurately described and actually support a ruling in favor of the Appellant.

First, citing *McKethean*, 588 A.2d at 708 as “holding that decisions relating to “traffic and safety design” were discretionary” is broader than it was. More accurately, the *McKethean* court held that “the decision to relocate a bus stop” was discretionary. *McKethean*, 588 A.2d at 715. Even after coming to this conclusion, the *McKethean* court expressly found that if there had been an “affirmative act of negligence, such as allowing the bus stop to deteriorate” such facts “might give rise

to liability.” *McKethean*, 588 A.2d at 716 (citing *Wagshal v. District of Columbia*, 216 A.2d 172 (D.C. 1966) (negligent failure to maintain a stop sign)). Moreover, citing *Berkovitz*, the court noted that there were no applicable “statutes or regulations which would limit the discretion of the District in relocating bus stops. *Id.* (citing *Berkovitz*, 486 U.S. at 536). The instant case, unlike *McKethean*, involves *both* negligence and a relevant statute that limited the discretion of the District.

In *Nealon* and *Chandler*, the cases related to **policy** decisions associated with maintenance of fire protection systems. But unlike the instant case, *Chandler* and *Nealon* involved policy decisions that were not subject to any specific statutory requirement. Moreover, there was no affirmative negligence or omission in the institution of the fire protection policies. The instant case, in contrast, is subject to a statutory obligation and the Plaintiff makes numerous allegations about the District’s negligence and omissions related to the District’s statutory obligations.

Under any analysis, the law is clear that the privilege of immunity is not available to the District in this case. The Court’s ruling that sovereign immunity applies should be reversed.

CONCLUSION

The ruling must be overturned as a radical departure from existing case law and as a matter of public policy. Cyber security must not be treated as a “black box” that cannot be broken into its component parts and be understood. Cyber security is

a critical function that citizens of the District of Columbia all increasingly rely upon in their day to day lives, no less than we use roads and sewers. The government must be accountable for its cyber security within the construct of existing law instead of being given an impenetrable shield that protects it from any act of negligence against those who rely upon it for safety and security. The Dismissal Order must be reversed.

* * *

Respectfully submitted,

/s/Arnold J. Abraham

*Arnold J. Abraham, Esq. (DC Bar No. 90003838)

CyberLaw, LLC

220 N. Liberty Street

Baltimore, MD 21201

Phone: 443-906-3495

/s/Eric J. Menhart

Eric J. Menhart, Esq. (DC Bar No. 975896)

Lexero Law

512 C St NE

Washington, D.C. 20002

Phone: 855-453-9376

STATEMENT AS TO TYPEFACE

The font used in this Brief is Times New Roman and the type size is 14 point.

/s/ Eric Menhart

Eric J. Menhart

CERTIFICATE OF SERVICE

I hereby certify that on January 3, 2023, a copy of the foregoing was delivered via the Court's electronic case filing system.

/s/ Eric Menhart

Eric J. Menhart

District of Columbia Court of Appeals

REDACTION CERTIFICATE DISCLOSURE FORM

Pursuant to Administrative Order No. M-274-21 (filed June 17, 2021), this certificate must be filed in conjunction with all briefs submitted in all cases designated with a “CV” docketing number to include Civil I, Collections, Contracts, General Civil, Landlord and Tenant, Liens, Malpractice, Merit Personnel, Other Civil, Property, Real Property, Torts and Vehicle Cases.

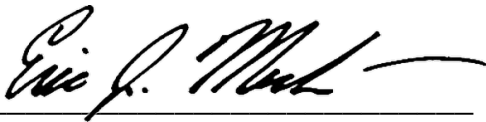
I certify that I have reviewed the guidelines outlined in Administrative Order No. M-274-21 and Super. Ct. Civ. R. 5.2, and removed the following information from my brief:

1. All information listed in Super. Ct. Civ. R. 5.2(a); including:

- An individual’s social-security number
- Taxpayer-identification number
- Driver’s license or non-driver’s’ license identification card number
- Birth date
- The name of an individual known to be a minor
- Financial account numbers, except that a party or nonparty making the filing may include the following:

- (1) the acronym “SS#” where the individual’s social-security number would have been included;
- (2) the acronym “TID#” where the individual’s taxpayeridentification number would have been included;
- (3) the acronym “DL#” or “NDL#” where the individual’s driver’s license or non-driver’s license identification card number would have been included;
- (4) the year of the individual’s birth;
- (5) the minor’s initials; and
- (6) the last four digits of the financial-account number.

2. Any information revealing the identity of an individual receiving mental-health services.
3. Any information revealing the identity of an individual receiving or under evaluation for substance-use-disorder services.
4. Information about protection orders, restraining orders, and injunctions that “would be likely to publicly reveal the identity or location of the protected party,” 18 U.S.C. § 2265(d)(3) (prohibiting public disclosure on the internet of such information); *see also* 18 U.S.C. § 2266(5) (defining “protection order” to include, among other things, civil and criminal orders for the purpose of preventing violent or threatening acts, harassment, sexual violence, contact, communication, or proximity) (both provisions attached).
5. Any names of victims of sexual offenses except the brief may use initials when referring to victims of sexual offenses.
6. Any other information required by law to be kept confidential or protected from public disclosure.



Signature

Eric Menhart, Esq,

Name

Eric.Menhart@Lexero.com

Email Address

22-CV-760

Case Number(s)

01/3/2023

Date