The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE and TIM JANECYK, for themselves and others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

No. 2:20-cv-01082-JLR

PLAINTIFFS' OPPOSITION TO DEFENDANT MICROSOFT CORPORATION'S RENEWED MOTION FOR SUMMARY JUDGMENT

ORAL ARGUMENT REQUESTED

INTRODUCTION

Far from meeting its burden on summary judgment, Defendant's "evidence" and the discovery taken so far establishes that: 1) Defendant downloaded the Diversity in Faces ("DiF Dataset") on at least two occasions; 2) Defendant's uses of the DiF Dataset were substantial, including but not limited to using metadata contained in the dataset, downloading all of the 1 million photographs linked to therein, running its facial recognition technology on a subset of those faces, and potentially using it evaluate another facial recognition system it was looking to acquire; 3) in both instances, the individuals downloading the DiF Dataset most likely stored it in Illinois and Texas; and 4) Plaintiffs reside in Illinois, and Defendant's corresponding invasion of their privacy and the harms resulting therefrom all occurred in Illinois.

Against this background, Defendant boldly moves for summary judgment, contending that *no evidence* supports Plaintiffs' position with respect to its arguments on extraterritoriality, the Dormant Commerce Clause, Section 15(b) of BIPA, and unjust enrichment. Not so. The Court should deny the first three bases of Defendant's motion for the same reasons it rejected them when Defendant first raised them in its motion to dismiss (Dkt. 25), and because the record's development since then only strengthened Plaintiffs' already superior position. Even assuming the Court need to delve into where the DiF Dataset was obtained and kept (which Plaintiffs maintain is unnecessary), at *best*, Defendant has showed a genuine issue of material fact as to whether this occurred in Illinois, and Plaintiffs' uncontested Illinois residency tips the scale in their favor. At worst, the evidence establishes that the datasets were stored in Illinois, which, in connection with Plaintiffs' undisputed Illinois' residency, also doom's Defendant's extraterritoriality and Dormant Commerce Clause Arguments. Defendant has also failed to meet its burden with respect to unjust enrichment, as the evidence creates a disputed question of material fact as to whether Defendant actually used the DiF Dataset for its intended purpose (determining whether to acquire the facial recognition system it was evaluating).

FACTUAL BACKGROUND

A. Plaintiffs' Photographs Appear in the DiF Dataset

Plaintiffs Steven Vance and Tim Janecyk ("Plaintiffs") have lived in Chicago, Illinois since approximately 2006 and in Tinley Park, Illinois since 1999, respectively. Ex. 1[1] (Vance Dep. Tr.) at 9:15-10:9. Ex. 2 (Janecyk Dep. Tr.) at 39:7-40:1. At relevant times, Vance and Janecyk had Flickr accounts to which they uploaded approximately 37,000 and 15,000 photos, respectively. Ex. 1 (Vance Dep. Tr.) at 120:9-22:9, 255:1-7.; Ex. 2 (Janecyk Dep. Tr.) at 44:9-11, 49:16-50:11. Flickr is a website to which users can upload photos. Ex. 3 (Verizon Dep. Tr.) at 34:24-35:19. Included in Plaintiffs' Flickr photos and those at issue here were photos they took in Illinois. Ex. 4 (Vance Interrog. Ans.) at Nos. 1-2; Ex. 5 (Vance Chicago photo) at 3-4; Ex. 1 (Vance Dep. Tr.) at 153:4-16; Ex. 6 (Janecyk Interrog. Ans.) at Nos. 1-2; Ex. 2 (Janecyk Dep. Tr.) at 97:14-20. It was each Plaintiff's habit or routine practice to upload photos to his Flickr account from his home in Chicago and Tinley Park, Illinois, respectively. Ex. 1 (Vance Dep. Tr.) at 255:8-16; Ex. 2 (Janecyk Dep. Tr.) at 81:13-21, 97:21-98:1. Plaintiffs restricted the use of the photos they uploaded to Flickr in two ways: (a) via a Creative Commons license; and (b) limiting who could view the photos online. *See* Ex. 1 (Vance Dep. Tr.) at 75:17-76:19, 206:1-21; *See* Ex. 2 (Janecyk Dep. Tr.) at 49:16-50:11, 100:18-102:3, 138:4-24. The Creative Commons license restricted the ways in which others could use Plaintiffs' photos. *See* Ex. 1 (Vance Dep. Tr.) at 75:17-76:19; Ex. 7 (Vance Creative Commons license); Ex. 8 (Janecyk Creative Commons license) Specifically, Plaintiffs prohibited commercial use of their photos, required those using their photos to provide attribution credit and provide a link to the license, and required anyone sharing their photos to share them under the same license. *See id.*

Notwithstanding BIPA's provisions, at no time did Defendant provide written notice to Plaintiffs that it intended to obtain their Biometric Data from their Flickr photos, nor did it obtain their written consent to do so. *See* Ex. 9 (Defendant's Supp. Interrog. Ans.) at No. 3 (setting forth

[1] Unless otherwise noted, all citations to exhibits are to those exhibits attached to the Lange Declaration, attached hereto as Exhibit A.

reasons Defendant did not comply with BIPA); Ex. 10 (Defendant's Interrog. Ans.) at No. 4 (attempting to explain why Defendant was not required to provide notice or obtain consent); Ex. 1 (Vance Dep. Tr.) at 58:17-19, 93:6-94:4, 190:3-12, 201:14-202:18; Ex. 4 (Vance Interrog. Ans.) at Nos. 1-2; Ex. 2 (Janecyk Dep. Tr.) at 121:8-14, 121:18-21, 135:15-21, 178:22-179:2; Ex. 6 (Janecyk Interrog. Ans.) at Nos. 1-2.

B. Benjamin Skrainka's Download, Storage, and Use of the DiF Dataset

Benjamin Skrainka worked for Defendant as a subcontractor from September 7, 2018 through August 1, 2019 to assist Microsoft [redacted]. Ex. 11 (Skrainka Dep. Tr.) at 91:15-24; 111:19-23; 122:14-123:18; Ex. 12 [redacted] Specifically, Mr. Skrainka's goal was to compute metrics to evaluate the performance of facial recognition technologies, including Microsoft's own facial recognition products, and to assist Microsoft in its decision as to [redacted]. Ex. 11 (Skrainka Dep. Tr.) at 106:14-24; 122:14-123:14; 127:3-20; Ex. 12 [redacted]

On February 1, 2019, Mr. Skrainka emailed IBM requesting access to the IBM DiF dataset. Ex. 13 (Skrainka/Microsoft DiF Request Questionnaire); Ex. 11 (Skrainka Dep. Tr.) at 198:14-22; 202:17-203:4). On February 16, 2019, IBM approved Mr. Skrainka's request and sent him the URL link to a file containing the DiF dataset. Ex. 14 (Skrainka-IBM Email Chain); Ex. 11 (Skrainka Dep. Tr.) at 216:4-217:16. After downloading the DiF Dataset, Mr. Skrainka wrote and ran a program that additionally downloaded each of the approximately 1 million URLs linking Flickr photographs to Defendant's cloud storage. *Id.* at 243:16-245:2. He spent two to four hours actively working on the DiF Dataset, but the program he ran took approximately two days or a week to run. *Id.* at 247:15-248:10. Mr. Skrainka also isolated and oriented approximately 100 to 1,000 faces appearing in the DiF Dataset, using their corresponding metadata, and ran Defendant's facial recognition software on them. *Id.* at 135:15-136:9; 230:3-15; 234:6-9.

Mr. Skrainka believed that the "vast majority" of the images in the DiF Dataset didn't function well when fed through the face recognition service, which he assumed was because the

images were unconstrained (i.e., of various poses and angles). *Id*. at 250:21-252:4. Mr. Skrainka does not recall what dataset he eventually used to evaluate AnyVision and cannot recall whether it was the DiF Dataset. *Id*. at 356:4-22. He was working with the DiF Dataset during Phase IV of his work, which is when he was evaluating AnyVision. *Id*. 340:19-341:3. He can only recall using two other datasets for this project: IJB-C, which was not an ideal dataset to test AnyVision because (like the DiF Dataset) it did not have sufficient constrained images and video data; and a dataset from the Balkans that was less helpful than the DiF Dataset. *Id*. at 139:4-19; 254:16-255:17; 345:19-346:7. One document Mr. Skrainka researched and wrote, which neither he nor Defendant could locate, likely contained several of Mr. Skrainka's findings concerning the datasets he was working with, including the DiF Dataset. *Id*. at 326:5-23; Ex. 15 (May 11, 2022 Email). Mr. Skrainka admits that others could have had access to the DiF Dataset while it was stored in Defendant's cloud and that he would not have known if they had. *Id*. at 362:14-363:24.

1. Mr. Srainka's Storage of the DiF Dataset

Evidence with respect to where Skrainka saved the DiF Dataset is contested and contradictory. In March 2019, Mr. Skrainka responded to a subpoena for documents unequivocally stating that he performed all of his work in the cloud and that all data he obtained was loaded onto virtual machines and cloud storage. Ex. 16 (Skrainka Subpoena); Ex. 17 (Skrainka response) at SKRAINKA 000002. On December 14, 2020, Microsoft contradicted this, stating that its investigation "has revealed no record of the copy of the DiF Dataset downloaded by Mr. Skrainka ever being downloaded to or stored on any Microsoft storage devices or equipment, including servers." Ex. 10 (Defendant Interrog. Ans.) at No. 8.

On July 15, 2021, Microsoft supplemented its interrogatories to state that:

> "if *any copy* of the IBM DiF Dataset .csv file that Ms. Samadi and Mr. Skrainka downloaded […] *was ever stored on Microsoft servers in the cloud*[2] […]—a hypothetical scenario, as Microsoft has not been able to establish that either Ms. Samadi or Mr. Skrainka stored the dataset or any portion of it on any Microsoft services—that .csv file would have been chunked […] and encrypted, and the

[2] Mr. Kuttiyan also testified that information saved through Azure storage, regardless of whether it is saved via a virtual machine or Azure Blob Storage, is being saved via Microsoft Cloud. Ex. 18 (Kuttiyan Dep. Tr.) at 36:5-9.

> encrypted chunks would have been stored in data centers, likely in San Antonio, Texas, and Chicago, Illinois."

Ex. 9 (Defendant Supp. Interrog. Ans.) at No. 8.

On December 10, 2021, Defendant submitted Mr. Skrainka's declaration in support of its initial motion for summary judgment, declaring that, consistent with Defendant's Supplemental Interrogatory Answer, he did not recall specifically where he downloaded or saved the DiF Dataset if he saved it, or whether he saved it on a virtual disk on Defendant's virtual machines or to any other location in Microsoft's cloud, but that he only stored data in Microsoft's cloud infrastructure. Dkt. 87, ¶8.

On March 1, 2022, Mr. Skrainka testified at his deposition that he saved the DiF Dataset and his related work in Microsoft's cloud. Ex. 11 (Skrainka Dep. Tr.) at 143:1-4. He "speculated" that he used a West Coast availability zone (implying that the documents would be stored in a datacenter located on the west coast) because using a different availability zone would be slow, and that "Blob storage is always slow." *Id*. at 147:5-20. Mr. Skrainka noted that he may have saved data in other availability zones, including the East Coast Availability Zone. *Id.* at 148:15-17. Mr. Skrainka further acknowledged that his testimony is at odds with Microsoft's sworn supplemental interrogatory answer that data stored in its cloud would have been saved in Texas and Illinois. *Id*. at 148:5-17. Mr. Skrainka claims to have discussed with Defendant's counsel "frequently" (over twenty hours) and "confirmed and reconfirmed" this with them throughout the case. *Id*. at 21:8-22:1, 161:10-23. Nonetheless, Mr. Skrainka does not know why Defendant confirmed that data stored in the cloud would be located in Texas and Illinois and was unable to explain this discrepancy. *Id*. at 162:19-24; 163:8-14; 183:21-184:8.

On March 9, 2022, Mr. Skrainka testified at his continued deposition that he reviewed no further documents since his March 1, 2022 testimony. *Id*. at 308:21-309:17. Nonetheless, Mr. Skrainka testified in response to his own counsel's questioning that he reviewed "Microsoft documentation for setting up a Linux machine," which he found online but could not recall the website of, "and that made it pretty clear to me that [the DIF Dataset] would have been [saved to] a West coast machine." *Id*. at 372:10-373:3; 389:9-16. Mr. Skrainka refused to answer any

questions regarding this "Microsoft documentation" on the basis of attorney-client privilege, including even foundational questions such as why he reviewed this documentation, whether he printed it, and what, if anything, about the documentation purportedly led him to believe this. *Id*. at 388:10-389:1; 389:17-392:2.

On April 15, 2022, Defendant supplemented its interrogatory answers again based upon Mr. Skrainka's deposition testimony, this time providing that "it's almost surely the case" that Mr. Skrainka saved the DiF Dataset to a West Coast availability zone, and that such data would have been stored in servers located in Washington or California, contradicting its prior answers and Mr. Skrainka's declaration. Ex. 19 (Defendant Second Supp. Interrog. Ans.) at No. 8.

Defendant relies on Sirius Kuttiyan for the proposition that an Azure user selecting an Azure Availability Region in the west coast in February 2019 would be storing data in data centers located in Washington or California. Dkt. 128, ¶4. However, Mr. Kuttiyan confirmed that he has no idea whether Mr. Skrainka selected any availability region or, if he did, which region that may have been. Ex. 18 (Kuttiyan Dep. Tr.) at 58:22-59:14. Moreover, he has no personal knowledge of whether documents stored in the west coast availability zones were actually stored in west coast data centers, beyond the public webpage attached to his declaration and "discussions" in the "product teams," which he did not verify as being true or false. *Id*. at 52:7-53:21. He does not know who at Microsoft published the webpage and did not verify its accuracy. *Id*. at 53:22-56:17.

Nor did Mr. Skrainka know whether data he saved in the cloud was backed up in or migrated to another availability zone. Ex. 11 (Skrainka Dep. Tr.) at 151:19-24; 185:15-20. Mr. Kuttiyan confirmed that data may be backed up to datacenters in other availability zones, and how that is done depends on the choices users make in saving their data. Ex. 18 (Kuttiyan Dep. Tr.) at 62:17-63:4; 63:24-65:2. Mr. Kuttiyan does not know whether options existed in 2019 that allowed users to back up data in availability regions beyond "paired regions," or whether Mr. Skrainka employed any methods to back up his data. *Id*. at 67:10-17; 69:13-19; 70:7-23. Moreover, Defendant may back up data saved to regions within the United States to other regions in the United States where services require, and Mr. Kuttiyan does not know which services these are.

Id. at 73:1-74:9; Ex. 20 (Data Residency in Azure), at 2-3 [MSFT_00000660]. He has not personally investigated whether Defendant replicates this data for resiliency purposes. Ex. 18 (Kuttiyan Dep. Tr.) at 74:10-75:11.

2. Mr. Skrainka's Testimony and Declaration Are Unreliable

Mr. Skrainka refers to this lawsuit as "this unpleasantness" and has "a common interest to see this case dismissed" because "it continues to cost me money" and "it takes time from the quiet enjoyment of my life." Ex. 11 (Skrainka Dep. Tr.) at 50:13-51:1. He also confessed that he was "happy to help Microsoft" and has an interest, as Microsoft does, in "having this go away." *Id*. at 361:5-12. He stated that he was "happy to help" Defendant's attorneys, and to do that, he was willing to put information in his declaration that Defendant's counsel wanted him to include. *Id*. at 361:5-362:8. Skrainka prepared his declaration and testified at his depositions to help Defendant, and understood Defendant would use the declaration to prevail in this lawsuit. *Id*. at 365:1-10. Defendant's counsel—not Mr. Skrainka—was responsible for "all kinds of legal boilerplate" in the declaration. *Id*. at 31:17-22. Mr. Skrainka also believes that memory is "plastic and unreliable." *Id*. at 193:11-12.

Moreover, he admitted portions of his declaration were inaccurate. He conceded that he not only reviewed, but *used* metadata contained in the DiF Dataset when working with it, despite averring in his declaration that he "ignored all metadata." *Id*. at 230:3-15; 376:23-385:1 (testifying that this statement was "5% false"); Dkt. 87, ¶6. Mr. Skrainka also testified that he knew certain information, including facial annotations, was included in the DiF Dataset before he downloaded it, despite averring in his declaration that he was not aware of this information. *Id*. at 209:10-17; 211:10-13; 211:14-212:24; Dkt. 87, ¶6. Likewise, his declaration states that he downloaded the DiF Dataset in "early February," when he in fact did not download it until at least February 16, 2019. *Id*. at 364:4-23; Dkt. 87, ¶5. As set forth *supra*, his deposition testimony contradicted both his declaration and Defendant's sworn interrogatory answers regarding his storage of the DiF Dataset.

C. Samira Samadi's Download, Storage, and Use of the DiF Dataset

From January 22, 2019 to May 3, 2019, Ms. Samadi worked as an intern at Microsoft Research. Ex. 21 (Samadi Dep. Tr.) at 17:4-12; Dkt. 88, ¶ 2. The goal of Ms. Samadi's work was "to measure how...human[] judgments of face similarities are affected by perceived race, skin tone, and gender of the faces they are shown." Dkt. 88, ¶ 2. During that work, Microsoft required Ms. Samadi to search for, download, access, and use a number of datasets containing diverse facial images, including the DiF Dataset. Ex. 21 (Samadi Dep. Tr.) at 60:13-61:14. Microsoft employees Hannah Wallach and Jennifer Wortman Vaughan supervised Ms. Samadi during her internship and recommended that she download the DiF Dataset. *Id.* at 21:15-23; 110:2-12; Ex. 22 (Vaughan Dep. Tr.) at 27:12-28:3. Through conversations with her co-workers, the decision was made that Ms. Samadi would complete the IBM DiF Request Questionnaire using her Georgia Institute of Technology credentials, as opposed to with her Microsoft credentials. Ex. 21 (Samadi Dep. Tr.) at 149:5-150:10. Evidence implies that Defendant [redacted]. *See Id.* at 146:13-147:17; *see* [redacted]

Ms. Samadi testified that, consistent with her declaration, she has no specific recollection as to the location, or locations, where she stored work-related files during her internship, including the location she stored the DiF Dataset. Ex. 21 (Samadi Dep. Tr.) at 39:1-16; Dkt. 88, ¶6. However, Ms. Samadi confirmed possible locations to which she may have initially saved DiF, prior to it being transferred to the server residing in New York. These possible locations include: her Microsoft Research-issued laptop (Ex. 21 (Samadi Dep. Tr.) at 39:1-10), her personal Dropbox account (Ex. 21 (Samadi Dep. Tr.) at 54:3-5, 55:9-16), a Google Drive account used by the Microsoft Research team (Ex. 21 (Samadi Dep. Tr.) at 51:15-17), and/or her Microsoft-issued OneDrive account (Ex. 21 (Samadi Dep. Tr.) at 57:5-19; 70:1-10; 72:9-16; 200:18-201:2).

Microsoft does not know where Ms. Samadi saved the DiF Dataset prior to its being moved to the New York server. Ex. 9 (Def's 1st Supp. Interrog. Ans.) at No. 8; Ex. 19 (Def's 2nd Supp. Interrog. Ans.) at No. 8. Ms. Samadi testified that it is not likely that she initially saved the DiF

Dataset to Google Drive because any dataset she was using would "naturally" be too big to keep there, or her Dropbox online storage accounts. Ex. 21 (Samadi Dep. Tr.) at 52:6-18; 54:6-9.

Of these possibilities, the evidence indicates that Ms. Samadi most likely saved the DiF Dataset in her OneDrive account prior to being directed to move it to a server in New York, discussed *infra*. An email exchange between Ms. Samadi and Microsoft Senior Service Engineer, Jeffrey Chirico, confirms that Ms. Samadi stored the "big data sets" she downloaded in her OneDrive Account. *Id*. at 58:2-8, 60:8-12; *see* Ex. 24 (Samadi-Chirico Email Chain). Ms. Samadi sent an email to Mr. Chirico requesting that her OneDrive account be upgraded to "OneDrive Premium." (*Id.*). She explained to Mr. Chirico that she was required to download and look into "big data sets" as part of her work, and since her OneDrive account was full, she was inquiring about OneDrive Premium. *Id.*; Ex. 21 (Samadi Dep. Tr.) at 60:8-61:14; 62:13-16; 63:2-5. Ms. Samadi testified that it was possible that her OneDrive account became full, and she needed more storage space, in-part because she had stored the "big data sets," in her OneDrive account. Ex. 21 (Samadi Dep. Tr.) at 65:6-20. Ms. Samadi confirmed that the "big data sets" were diverse facial datasets that she downloaded for the same project for which she downloaded DiF. *Id*. at 60:13-61:14.

Mr. Chirico instead directed Ms. Samadi to store her data on a server located in New York (hereinafter, "NY server"), which she eventually did. *Id*. at 219:8-10; Dkt. 93, ¶ 2; Ex. 25 (Chirico Dep Tr.) at 24:13-17; *see also* Ex. 24 (Samadi-Chirico Email Chain). Although Ms. Samadi could not recall whether she transferred information from her Microsoft-issued laptop or OneDrive account to the NY server, this the same NY server that Defendant eventually found the DiF Dataset on. Ex. 21 (Samadi Dep. Tr.) at 224:12-17; 228:4–229:4; Ex. 9 (Defendant Supp. Interrog. Ans.) at No. 8; Ex. 19 (Defendant Second Supp. Interrog. Ans.) at No. 8. Although Ms. Samadi believes she may have initially saved the DiF Dataset to her laptop instead of OneDrive (Dkt. 88, ¶6), it is possible that her laptop was automatically uploading information to OneDrive. *Id*. at 57:1-19. Further, Ms. Samadi testifies interchangeably about her laptop and OneDrive cloud storage

account. *See Id*. at 51:24-52:9 (referring to her emails with Jeff Chirico describing her OneDrive account being full as "apparently the space on my laptop was becoming full").

Defendant confirmed that any information Ms. Samadi saved to the cloud—including her OneDrive account housing "big data sets"— were physically stored in San Antonio, Texas and Chicago, Illinois. Ex. 9 (Defendant Supp. Interrog. Ans.) at No. 8; Ex. 19 (Defendant Second Supp. Interrog. Ans.) at No. 8; *see also* Dkt. 127 at 18.

ARGUMENT

Summary judgment is appropriate only where "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 248 (1986). "A genuine issue of material fact exists 'if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.'" *Sierra Medical Svcs Alliance v. Kent*, 883 F.3d 1216, 1222 (9th Cir. 2018) (quoting *Anderson*, 477 U.S. at 248). Every reasonable factual inference must be drawn in favor of the party opposing the motion for summary judgment, from both direct and circumstantial evidence. *Coghlan v. Am. Seafoods Co. LLC.,* 413 F.3d 1090, 1095 (9th Cir. 2005).

When the moving party does not bear the burden of proof on an issue at trial, the moving party may discharge its burden of showing that no genuine issue of material fact remains, but to do so it must first demonstrate that "there is an absence of evidence to support the nonmoving party's case." *Pintos v. Pacific Creditors Assoc.*, No. 03-cv-5471, 2004 WL 7333706, *2 (N.D. Cal. Nov. 9, 2004) (citing *Celotext Corp. v. Catrett*, 477 U.S. 317, at 325 (1986). Only *if* the moving party carries its initial burden of production, must the nonmoving party produce evidence to support its claim or defense that there is a genuine issue for trial. *Allstate Prop. and Cas. Ins. Co. v. Strand*, No. 11-cv-1334, 2012 WL 2004994, at *3 (W.D. Wash. Jun. 5, 2012).

A. Plaintiffs' Claims Are Not Barred by the Extraterritoriality Doctrine or the Dormant Commerce Clause.

Defendant's principal argument is that Plaintiffs' claims fail because BIPA "does not apply to Microsoft's out-of-state conduct," and if it did, this would violate the Dormant Commerce

clause. Dkt. 127 at 10. These arguments closely mirror arguments Defendant advanced at the motion to dismiss stage, Dkt. 25, which this Court rejected. Dkts. 43, 47. No further developments in the factual record alter the validity of the Court's prior analysis—that these doctrines do not support judgment against Plaintiffs' claims as a matter of law.

Contrary to Defendant's self-serving narration, it has failed to meet its opening burden in demonstrating "an absence of evidence to support [Plaintiffs'] case." *See Pintos*, 2004 WL 733707, at *2. Because Defendant has failed to meet its burden, the burden does not shift to Plaintiffs to support their claim. *See Allstate Prop. And Cas. Ins. Co.*, 2012 WL 2004994, at *3. Defendant has failed to meet its burden because what little evidence resulted from its own investigation only proved that most relevant conduct occurred in Illinois. Defendant has tied itself in knots trying to figure out where Mr. Skrainka and Ms. Samadi downloaded (and thus, received) copies of the DiF Dataset. Now that the dust has settled, Defendant's efforts have only shown that both Mr. Skrainka and Ms. Samadi likely downloaded the dataset to a datacenter in Illinois.

Indeed, the evidence shows that, as discussed *supra*:

- In March 2019, Mr. Skrainka first asserted that he stored all information on Microsoft's cloud;
- On December 14, 2020, Defendant confirmed via sworn interrogatory answers that it could find no record of DiF stored in its cloud;
- On July 15, 2021, Defendant confirmed via sworn interrogatory answers that if either Mr. Skrainka or Ms. Samadi saved the DiF Dataset to its cloud, it would have been stored in its datacenters in Illinois and Texas;
- On December 10, 2021, Defendant submitted Mr. Skrainka's sworn declaration stating that he could not recall where or how he saved the dataset, but that it was saved to Defendant's cloud;
- On March 1, 2022, Mr. Skrainka testified at his deposition that he probably saved the dataset to Defendant's cloud to either West coast or East coast datacenters;
- On March 9, 2022, Defendant testified at his continued deposition that he reviewed an unknown webpage that "made it pretty clear" that he would have saved the dataset to a West coast datacenter;
- On April 15, 2022, Defendant supplemented its interrogatory answers *again*, providing "it's almost surely the case" that Mr. Skrainka saved the dataset to a west

> coast datacenter, while maintaining that if Ms. Samadi saved the dataset to the cloud, it would have been stored in Illinois and Texas.

See Factual Background, Section B(1). Mr. Skrainka's abrupt departure at his deposition from his own sworn declaration and Defendant's sworn discovery responses is particularly disingenuous given his concession that his goal in writing his declaration and testifying at his depositions was to help Defendant's lawyers, that he wants this case dismissed because it costs him money and "takes time from the quiet enjoyment of my life." *See* Factual Background, Section B(2).

These head-spinning inconsistencies alone create a question of material fact as to whether Mr. Skrainka saved the DiF Dataset to Illinois. *See Koninklijke Philips Elec. N.V. v. Cardiac Sci. Operating Co.*, No. 08-cv-543, 2010 WL 5058405, at *2 (W.D. Wash. Dec. 6, 2010) (summary judgement improper when defendant's position on the issue changed from the initial claim to the motion for summary judgement); *Fireman's Fund Ins. Co. v. Thien*, 8 F.3d 1307, 1312 (8th Cir. 1993) (inconsistent statements from Defendant on material issue of fact could defeat a summary judgement motion); *Bollard v. Volkswagen of America, Inc.*, 56 F.R.D. 569, 575 (W.D. Mo. 1971) (contradictory answers on material facts construed as an attempt to change the record and influence the court's ruling on a motion); *Mullins v. Cyranek*, No. 1:12CV384, 2014 WL 3573498, *2 (S.D. Ohio July 21, 2014) (party moving for summary judgement cannot extinguish an issue of material facts by contradicting previous testimony); *See also Coleman v. S. Pac. Transp. Co.*, 997 F.Supp 1197, 1201 (D. Ariz. 1998).

While Defendant is unsure where Ms. Samadi initially kept the dataset, but believes she "probably" saved it to her laptop, the evidence demonstrates that she is most likely to have saved the dataset to her OneDrive account in the cloud, which was where she was saving other large datasets she was using for the same project. Even if she did save the dataset to her laptop, she has testified about her laptop and her laptop's OneDrive storage account interchangeably, and does not recall whether OneDrive was automatically backing up documents on her laptop to Defendant's cloud. *See* Factual Background, Section C. Defendant does not dispute that, if saved to the Cloud, the dataset would have been stored in Chicago and Illinois. Ex. 9 (Defendant's Supp. Interrog. Ans.) at No. 8; Ex. 19 (Defendant's 2nd Supp. Interrog. Ans.) at No. 8.

This is to say nothing of the only *truly* uncontested facts of this case, *infra*: Plaintiffs' Illinois residency and the corresponding invasion of privacy and harms occurring in Illinois.[3]

1. The Factual Record Demonstrates the Propriety of the Court's Prior Ruling.

In denying Defendant's motion to dismiss on the basis of extraterritoriality, this Court held that dismissal was inappropriate because:

> Plaintiffs, and all purported class members, are Illinois residents who, while in Illinois, uploaded photos that were taken in Illinois. The required disclosures or permissions would have been obtained from Illinois, and so any communication would have necessarily involved Illinois. The alleged harm to privacy interests is ongoing for Illinois residents. Moreover, Plaintiffs allege that Microsoft conducts "extensive business" in Illinois involving their facial recognition products, and that the Diversity in Faces dataset "improve[d] its facial recognition products," thereby allowing the reasonable inference that Microsoft utilized the dataset in Illinois during its business dealings.

Each of the allegations quoted above, found sufficient by the Court to preclude dismissal at the pleadings stage on the basis of extraterritoriality, are similarly supported by the summary judgment record, when viewed in the light most favorable to Plaintiffs. Plaintiffs are Illinois residents who, "while in Illinois," uploaded photos taken in Illinois. *See* Statement of Facts, Section A. Had Defendant made any effort to comply with BIPA, the communications would have necessarily involved Illinois. Defendant downloaded the DiF Dataset on two occasions in an effort to further develop its facial recognition technologies, and Mr. Skrainka likely used the DiF Dataset to evaluate [redacted]. Ex. 11, (Skrainka Dep. Tr.) at 356:4-22. Additionally, discovery has shown that both copies of the DiF Dataset Defendant possessed were likely stored in Illinois. *See* Ex. 9 (Defendant Supp. Interrog. Ans.) at No. 8; Ex. 19 (Defendant 2nd Supp. Interrog. Ans.) at No. 8. Moreover, as the Court also found previously, the geographic location "where Microsoft obtained the dataset . . . may not be dispositive." Dkt. 43 at 8. Defendant does not argue that there has been any change in the

[3] This Court should also reject Defendant's argument that the location to which Mr. Skrainka and Ms. Samadi downloaded the DiF Dataset is irrelevant because Section 15(b) only applies to the acquisition, not storage, of biometric data. Dkt. 127, at 18. Because Mr. Skrainka and Ms. Samadi would have downloaded the dataset *initially* to the cloud, the location of storage is the same as the location of acquisition. Regarding, the location of the dataset while Defendant used it is relevant.

controlling law, and its citation to a single outlier out-of-circuit case demonstrates there has been none. Nor are there any other factors that would warrant a departure from the court's prior ruling. The Court's prior determination of the applicable legal rule, applied to the record, shows that Defendant is not entitled to summary judgment.

2. Illinois law demonstrates that Plaintiffs' claims do not require extraterritorial application of BIPA

Regardless, even if it had not already decided this issue, this Court should find that Plaintiffs' claims do not require the extraterritorial application of BIPA. In *Avery v. State Farm Mut. Auto. Ins. Co.,* 835 N.E.2d 801, 854 (Ill. 2005), the Illinois Supreme Court provided a detailed discussion of the extraterritoriality principles that apply when determining the proper reach of an Illinois statute. While "[t]here is no single formula or bright-line test for determining whether a transaction occurs within this state[,]" the court determined that some relevant circumstances in determining whether alleged fraudulent consumer transactions occurred "primarily and substantially" within Illinois were: (a) where the plaintiffs resided; (b) where the deception or "failure to disclose" occurred; and (c) where the plaintiffs incurred their injury. 835 N.E.2d at 854.

Applying the *Avery* factors here, Defendant's summary judgment motion fails. Because Plaintiffs' Illinois residency is undisputed, this is not a case where the plaintiffs "are non-residents suing under Illinois law, which is the paradigmatic situation for the presumption against the extraterritorial application of local law." *In re Facebook Biometric Info. Privacy Litig*., 326 F.R.D. 535, 547 (N.D. Cal. 2018) (citing *Avery*, 835 N.E.2d 801).

Further, photos from which Plaintiffs' Biometric Data was collected were taken in Illinois and uploaded to the internet in Illinois. Statement of Facts, Section A. Similarly, had Defendant complied with the requirements of BIPA, the required notifications and consents would have taken place in Illinois. *See Rivera v. Google, Inc*., 238 F.Supp.3d 1088, 1102 (N.D. Ill. 2017) ("lack of consent" occurs where the person is located when deprived of the necessary information).

Finally, Plaintiffs' injuries occurred in Illinois. The Seventh Circuit has likened a defendant's collection of a victim's biometric data without providing notice and obtaining

"informed consent" to an invasion of the victim's "private domain, much like an act of trespass would be . . . ." *See Bryant v. Compass Grp USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020). That "invasion" or "trespass" occurs in Illinois, the location of the victim's "private domain." *See id.*

The strong consensus of courts which have decided this issue have found, as this Court did previously, that the extraterritoriality doctrine does not preclude BIPA's application to claims brought by Illinois residents relating to biometric data derived from photographs taken and uploaded to the internet in Illinois—regardless of the geographic location of the corporation which ultimately came into possession of the biometric information, or of the servers on which the data was stored. *See, e.g.*, *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 547 (N.D. Cal. 2018) ("There is no genuine dispute that this case is deeply rooted in Illinois. The named plaintiffs are located in Illinois along with all of the proposed class members, and the claims are based on the application of Illinois law to use of [social media site] mainly in Illinois."); *In re Clearview AI, Inc., Consumer Priv. Litig.*, 2022 WL 444135, at *4 (N.D. Ill. Feb. 14, 2022) (holding Illinois residents who were deprived of BIPA-compliant notices in Illinois, resulting in privacy violations in Illinois, did not require extraterritorial application of BIPA, despite defendant's claim that it created its biometric database in New York); *Rivera*, 238 F. Supp. 3d at 1101-02 ("Illinois connections" consisting of plaintiffs' Illinois residency, Illinois upload of photographs taken in Illinois, and failure to provide notice and obtain consent in Illinois, all suggest that alleged violations "primarily happened in Illinois," regardless of the location of the face scan generating the biometric data); *cf Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017) (finding sufficient facts that could defeat extraterritoriality argument even for non-Illinois resident plaintiff, where photograph was uploaded in Illinois by Illinois citizen and required notice/consent would have been occurred in Illinois).

Defendant's extraterritoriality defense falls particularly flat "in light of BIPA's express concerns about data collection by '[m]ajor national corporations,'" which appropriately colors the Court's analysis of the issue. *Id.* (noting that territoriality inquiry looks to the "objects of the statute's solicitude"). *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. at 547.

Defendant's Motion focuses almost entirely on the geographic location of its employees at the time they downloaded, accessed, and analyzed the biometric information contained within the DiF dataset. Dkt. 127 at 15-20. However, this is far from dispositive. In analyzing a similar BIPA claim, the Ninth Circuit held that "it is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019). Moreover,

> [m]aking the geographic coordinates of a server the most important circumstance in fixing the location of an Internet company's conduct would yield the questionable results *Avery* counsels against. Among other problematic outcomes, it would effectively gut the ability of states without server sites to apply their consumer protection laws to residents for online activity that occurred substantially within their borders.

In re Facebook Biometric Info. Priv. Litig., 326 F.R.D. at 548.

3. Defendant's Reliance on McGoveran is unpersuasive.

Defendant relies principally on *McGoveran v. Amazon Web Servs., Inc.*, 2021 WL 4502089, at *1 (D. Del. Sept. 30, 2021), an outlier case from the District of Delaware. This Court need not and should not follow *McGoveran*, in light of its own prior ruling and the clear consensus of the remaining case law. However, even if it found *McGoveran* persuasive, *McGoveran* does not compel judgment in Defendant's favor. In *McGoveran,* Amazon's alleged role in the claimed BIPA violation was simply that biometric data was stored on its servers, and scanned by one of its customers using Amazon's cloud-based call center services. *McGoveran*, 2021 WL 4502089 at *1. Unlike *McGoveran*, here, Defendant actively obtained and used Plaintiffs' Biometric Data for its own benefit in Illinois.

While the court in *McGoveran* did not consider the location where the Defendant was required to provide notice and obtain consent, that aspect of the decision is unpersuasive. As a threshold matter, the Illinois Supreme Court has expressly held that the location of an allegedly unlawful *failure to communicate* with a consumer is an important part of the extraterritoriality analysis. *See Avery*, 835 N.E.2d at 854 (finding claims of non-Illinois resident barred by extraterritoriality doctrine because "[t]he alleged deception in this case – the failure to disclose"

certain facts about automobile parts, occurred in Louisiana, not Illinois). Further, as discussed above, various other federal courts have reached a different conclusion than the court in *McGoveran*. Moreover, it would be absurd to permit "major national corporations" like Defendant, expressly the target of BIPA's intended reach, *see* 740 Ill. Comp. Stat. 14/5(b), to evade BIPA's carefully crafted privacy protections for Illinois residents, simply by avoiding contact with the very citizens the statute seeks to protect.

B. The Dormant Commerce Clause does not Bar Plaintiffs' Claims.

While the Dormant Commerce Clause limits states' powers, "[n]ot every exercise of state power with some impact on interstate commerce . . . violates the Commerce Clause." *Gravquick A/S v. Trimble Navig. Int'l Ltd.*, 323 F.3d 1219, 1224 (9th Cir. 2003). The Supreme Court has developed a two-pronged test to determine whether a state economic regulation violates the Commerce Clause. *See Chinatown Neighborhood Ass'n v. Harris* ("*Chinatown*"), 794 F.3d 1136, 1145 (9th Cir. 2015). If a state statute discriminates against or directly regulates interstate commerce, a court should strike down the statute (or challenged application thereof) without additional inquiry. *Id.* However, where a statute only has an indirect effect on interstate commerce, no Dormant Commerce Clause violation exists unless the statute's burdens outweigh its putative benefits, making it irrational or unreasonable. *Id.*

A statute "directly regulates" interstate commerce and violates the Commerce Clause where it directly controls commerce taking place *wholly* outside a state's boundaries. *Rocky Mountain Farmers Union v. Corey,* 730 F.3d 1070, 1101 (9th Cir. 2013). But if a statute regulates a transaction or relationship "in which at least one party is located in [the regulating state]," as with BIPA, the statute does not regulate extraterritorial conduct for purposes of the "direct regulation" test. *Chinatown*, 794 F.3d at 1146. Indeed, BIPA's legislative history makes clear that, far from being directed to commerce *wholly* outside of Illinois, the law was enacted arising from the Illinois General Assembly's concern with out-of-state entities reaching *into* Illinois to engage in novel uses of biometric technology—uses which, without appropriate safeguards, risked compromising the sensitive private data of Illinois residents. *See* 740 ILCS 14/5(b), (c), (g) (noting

that "[m]ajor national corporations" are using Illinois communities "as pilot testing sites for new applications of biometric-facilitated" transactions; finding that biometrics are uniquely sensitive which, "once compromised," leave an individual with "no resource;" and enacting provisions to regulate and safeguard the collection, use, and handling of biometric identifiers and information).

States have broad power to enact laws that protect their residents in matters of local concern. *Nat'l Ass'n of Optometrists and Opticians v. Harris*, 682 F.3d 1144, 1148 (9th Cir. 2012). A state "may regulate with reference to local harms" even if the regulation impacts out-of-state entities whose conduct has in-state ramifications. *Corey*, 730 F.3d at 1104. Furthermore, the Dormant Commerce Clause does not demand uniformity among state laws. *Corey*, 730 F.3d at 1104. "If we were to invalidate a regulation every time another state considered a complementary statute, we would destroy the states' ability to experiment with regulation." *Id.* at 1105.

BIPA's application to Defendant's obtainment and use of Plaintiffs' biometric information for its own pecuniary benefit does not violate the 'direct regulation' prong of the Dormant Commerce Clause test, because BIPA does not control commerce wholly outside of Illinois. And given the practical realities of commerce in the digital age, the Supreme Court has held that it is inappropriate to "limit[] the lawful prerogatives of the States" by requiring that regulated entities have a physical presence in the state. *South Dakota v. Wayfair, Inc.*, 138 S. Ct. 2080, 2097 (2018).

Defendant makes no argument at all that is addressed towards the second prong of the test, requiring a finding that the statute's burdens outweigh its putative benefits, making it irrational or unreasonable in order to find a Dormant Commerce clause violation. *Chinatown,* 794 F.3d at 1145. The point is therefore waived. *Fox v. Holland Am. Line, Inc.*, 2016 WL 258522, at *3 (W.D. Wash. Jan. 21, 2016). And wisely so, since at the summary judgment stage, with all evidence construed in Plaintiffs' favor, the putative benefits of protecting Illinois residents' privacy would outweigh any purported burden resulting from Defendant's compliance with the statute. *See Ades v. Omni Hotels Mgm't Corp.*, 46 F.Supp.3d 999, 1015-16 (C.D. Cal. 2014) (finding no Dormant Commerce Clause violation where California privacy statute required out-of-state call center to identify calls from California).

Instead of addressing the second prong of the test, Defendant asserts that applying BIPA is unlawful because it would "conflict with" the policy decisions of Washington and New York in enacting different (or non-existent) state statutory schemes regarding biometric data. Dkt. 127 at 24-26. The argument is unpersuasive. First, there is no conflict. Defendant does not allege that compliance with its obligations under Illinois' BIPA statutes would compel it to violate its state law obligations in Washington or New York— it simply points out that BIPA imposes more stringent requirements than these other states (but which are alleged to apply in this case only with reference to Illinois residents).

The existence of two state statutes that regulate biometric data does not offend the Dormant Commerce Clause. *See Corey,* 730 F.3d at 1105. As the Ninth Circuit has recognized, "[s]uccessful [state regulatory] experiments inspire imitation both vertically . . . and horizontally . . . . ." *Id.* at 1105. Thus, "[i]f we were to invalidate regulation every time another state considered a complementary statute, we would destroy the states' ability to experiment with regulation." *Id.*

Illinois' and Washington's biometric law are complementary—*i.e.*, they both seek to shape the confines of the appropriate use of Biometric Data. *See* 740 ILCS 14/1, *et seq.*; RCW 19.375.010, *et seq.* These states' experimentation with regulation does not require that either state's statute be invalidated; nor does it allow Washington to render BIPA meaningless vis-à-vis Washington private entities' relationships with Illinois residents. At once, Defendant complains of BIPA's reach, while also seeking to impermissibly project Washington's regulatory scheme onto Illinois and negate BIPA's privacy protections. *Cf. In re Facebook Biometric Info. Privacy Litig.*, 185 F.Supp.3d 1155, 1169-70 (N.D. Cal. 2016) (rejecting California choice of law provision that would negate BIPA's protections). If Washington were to pass a law exempting businesses from liability arising from the collection of Biometric Data, according to Defendant, Illinois could not exercise its legitimate interest in protecting its residents' privacy vis-à-vis Washington businesses.

Notably, the two cases that Defendant cites in support of its argument have nothing to do with the balancing required under the second prong of the Dormant Commerce Clause test. In *Nat'l Collegiate Athletic Ass'n v. Miller*, 10 F.3d 633, 639 (9th Cir. 1993), the Ninth Circuit Court

rejected a state statute imposing minimal procedural requirements for enforcement proceedings in collegial athletics, on the basis that "the serious risk of inconsistent obligations wrought by the extraterritorial effect of the [s]tatute demonstrates why it constitutes a per se violation of the Commerce Clause." *Id.* The concerns regarding the national collegiate organization at issue in *Miller* do not exist here, and *Miller* offers no support for the idea that BIPA's application fails the balancing test at the second step. *Miller* is also inapposite since the Plaintiffs do not seek to give BIPA extraterritorial effect. In *Mazza v. Am. Honda Co., Inc.*, 666 F.3d 581, 592 (9th Cir. 2012), the second case on which Microsoft relies, the court tackled a conflict of laws issue at class certification in a proposed nationwide class action where only one-fifth of the class members resided in the state whose legal framework was invoked as the basis for the claims, *id.*—a non-issue in this case since Plaintiffs and the entire class are Illinois residents.

B. BIPA Section 15(b) Applies to Microsoft's Download, Storage, and Use of the DiF Dataset.

This Court should reject Defendant's invitation to violate the 'law of the case' doctrine by changing its prior ruling on Defendant's same argument in the same case. Dkt. 43 at 26-27. This and other District Courts have ruled that Section "15(b) applies when a private entity collects, captures, trades for, *or gets biometric data in some other way*," even if the private entity does not have a preexisting relationship with the subjects it captured the biometric data from. Dkt. 43, at 19 (emphasis added); *Vance v. Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1314 (W.D. Wash. 2021); *Flores v. Motorola Solutions, Inc.*, No. 1:20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021); *Monroy v. Shutterfly, Inc.*, No. 16-cv-10984, 2017 WL 4099846, at *1 (N.D. Ill. Sep. 15, 2017); *Ronquillo v. Doctor's Associates, LLC*, No. 21-cv-4903, 2022 WL 1016600, at *3 (N.D. Ill. Apr. 4, 2022); *Figueroa v. Kronos, Inc.*, 454 F. Supp. 3d 772, 783-84 (N.D. Ill. 2020); *Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019).

In reiterating the same argument Defendant made before in its Motion to Dismiss (Dkt. 25, at 25-27), Defendant urges the Court to read imaginary limitations into BIPA allowing parties to freely obtain biometric data from Illinois residents so long as there is no preexisting relationship

with those Illinois residents. Dkt. 127, 26-28. In support, Microsoft relies on the misguided notion that it would be "practically impossible, to the point where application of Section 15(b) would be absurd," and on the uncited opinion issued in *Zellmer v. Facebook, Inc.*, 2022 WL 976981, at *3 (N.D. Cal. 2022).

First, this Court already refused to find that interpreting BIPA consistent with its plain language "does not, as Microsoft fears, produce an absurd result." *Microsoft*, at 1297-98. The Court explained:

> BIPA obligates any private entity that obtains a person's biometric identifier to comply with certain requirements to protect that person's privacy interests. *See* 740 ILCS 14/5 (recognizing public's wariness of use of biometrics and need for regulation for public welfare, security and safety). Whether that biometric information comes from an individual or is part of a large dataset, there is nothing absurd about requiring any entity that obtains such information to comply with the safeguards that the Illinois legislature deemed necessary. *See Neals*, 419 F. Supp. 3d at 1092; 740 ILCS 14/5(g). Although complying with BIPA requires entities like Microsoft to take additional steps before acquiring biometric data, the court does not believe that "under Plaintiffs' reading of the statute, no entity could safely download any large biometric dataset."

Dkt. 43, at 17-18. The Court also disposed of Defendant's prior caselaw, finding "[t]he same is not true here. To the extent that dicta in these cases require some relationship to exist, the court declines to adopt that interpretation, as that requirement does not appear in the statutory language, and persuasive authority exists to the contrary." *Id*. at 1298.

Nothing has changed since the Court first rejected this contention. As Plaintiffs contended previously, Defendant could have reached out to IBM *before* requesting the dataset, to confirm whether it contained photographs taken from Illinois and/or whether it contained the subjects' biometric data. If, as Defendant contends, its uses of the DiF Dataset did not require the biometric data included therein, Defendant could have requested a copy of the dataset with this protected data excluded. Or if Defendant wanted the biometric data, it could have undertaken any of the various methods proposed in Plaintiffs' Motion for Class Certification (Dkt. 70 at 25-28) to obtain consent of Illinois residents. Tellingly, Microsoft, either before or after obtaining the DiF Dataset did not attempt to contact any individual whose face appears in the DiF Dataset to obtain consent.

Of course, Defendant could have simply opted to *not* access this dataset containing biometric data in favor of using one that did *not* include biometric data. There is nothing absurd in requiring individuals to respect Illinois residents' sensitive biometric data if they choose to obtain it.

Defendant miscites to *Rosenbach v. Six Flags Ent't Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019) for the proposition that "'[c]ompliance should not be difficult' and any expense a business might incur to comply should be minimal." In *Rosenbach,* the Illinois Supreme Court made this assertion to emphasize compliance, not to minimize it. Nor did the Illinois Supreme Court ever indicate that "any expense a business might incur to comply should be minimal." Instead, the Court found that "whatever expenses a business might incur to meet the law's requirements are likely to be insignificant *compared to the substantial and irreversible harm that could result in biometric identifiers and information are not properly safeguarded*; and the public welfare, security, and safety will be advanced." *Id*. at 1207 (emphasis added). Defendant's efforts to comply with BIPA, if it had bothered to make any at all (e.g., obtaining a copy of the dataset with the biometric data omitted), would indeed be insignificant compared to the substantial and irreversible harm Defendant cast upon Illinois residents.

Nor should this Court follow the rationale in *Zellmer*, which has not been cited to and is an outlier to the extent its holding permits an entity to escape BIPA liability because it lacked a preexisting relationship with the Illinois resident from whom it collected biometric data. *Zellmer v. Facebook, Inc.,* 2022 WL 976981 (N.D. Cal. Mar. 31, 2022). In analyzing BIPA, the court in *Zellmer*, concluded that "the Illinois legislature clearly contemplated that BIPA would apply in situations where a business had at least some measure of knowing contact with and awareness of the people subject to biometric data collection." *Zellmer*, 2022 WL 976981, at *4; 740 ILCS 14/5(a)-(b). However, this rationale does not suggest that the state's legislature also intended to *exclude* from BIPA's purview the collection of biometric data in the absence of a preexisting relationship. Likewise, there is nothing in BIPA's language—including its references to various financial transactions—that evidences the Illinois Legislature's intent to that BIPA offers no protection in the absence of a preexisting relationship.

Indeed, Section 5(a)'s reference to financial transactions *and security screenings* explicitly encompasses the capture of biometrics from unknown individuals, including, for example, the use of facial recognition in connection with surveillance video on a street corner or in a shopping mall. 740 ILCS 14/5(a). This Court and the majority of others have refused to read such a limitation into BIPA. *See* Dkt. 43, at 17 ("Nor will the court adopt Microsoft's proposal that § 15(b) only applies when an entity acquires biometric data 'directly from any individual.' Nothing in the statute's language supports such a narrow application."); *Flores*, 2021 WL 232627, at *3 ("the requirement Defendants read into the statute does not appear in the statutory language itself. There is also persuasive authority that the statute applies where no relationship between the collector and the induvial exists."); *Ronquillo*, 2022 WL 1016600, at *3 ("more importantly, [defendants] cannot point to anything in BIPA's text that supports limiting § 15(b)'s reach only to employers."). This is no coincidence, as holding otherwise would effectively gut the statute's protections.

Regardless, this Court granting summary judgment based upon Defendant's implied limitation of Section 15(b) with respect to preexisting relationships is precluded by the law of the case doctrine and this Court's prior refusal to read this limitation into the Statute. Dkt. 43 at 26-27. In the Ninth Circuit, the "law of the case" doctrine precludes a court from "reconsidering an issue that has already been decided by the same court, or a higher court in the identical case." *U.S. v. Alexander*, 106 F.3d 874, 876 (9th Cir. 1997) (reversing district court for departing from law of the case); *G.G. v. Valve Corp.*, No. 2020 WL 7385710, at *6-7 (W.D. Wash. Dec. 16, 2020) (refusing to reconsider arguments in amended complaint that were already raised in the initial complaint and addressed by arbitrator's finding and the court's entry thereof). A court may have discretion to depart from the law of the case in certain instances not applicable here. *See Alexander*, 106 F.3d at 876. Failure to apply the doctrine of law of the case absent of the requisite conditions constitutes an abuse of discretion. *Id*. Because no such exceptions apply, the Court should not stray from its prior findings on this question.[4]

[4] Plaintiffs acknowledge that, in some circumstances, the Ninth Circuit Court allows district courts to reconsider their prior orders. *See U.S. v. Smith*, 239 F.3d 944, 949 (9th Cir. 2004). Regardless, this Court should not stray from its

C. The Court Should Deny Summary Judgment as to The Unjust Enrichment Claim.

This Court should deny summary judgment because a material question of fact exists as to whether Defendant profited from its use of the DiF Dataset. To prevail on unjust enrichment under Illinois law, Plaintiff must show that "[defendant] has unjustly retained a benefit to [the plaintiff's] detriment and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience." *Mabry v. Standard Industries, Inc.*, No. 20 C 376, 2020 WL 2112372, at *5 (N.D. Ill. May 4, 2020); *IBM*, 2020 WL 5530134, *5.

Undisputed evidence confirms that Microsoft obtained the DiF Dataset with the intent to use and profit from it. Specifically, Benjamin Skrainka downloaded the DiF Dataset to evaluate a facial recognition product that Microsoft was contemplating purchasing. Ex. 11 (Skrainka Dep. Tr.) at 250:21-252:4. He proceeded to use the DiF Dataset for this purpose. For example, Mr. Skrainka's work with the DiF Dataset spanned several days and involved downloading every image linked to in the DiF Dataset and running Microsoft's facial recognition technology on up to a thousand faces in the DiF Dataset. *Id*. at 243:16-245:2; 247:15-248:10; 135:15-136:9; 234:6-9. Despite this, and contrary to his declaration, Mr. Skrainka does not know which dataset he eventually used to evaluate AnyVision, and cannot recall whether it was the DiF Dataset, which he was working with during the time he was evaluating AnyVision. *Id*. at 356:4-22; 340:19-341:3. Neither he nor Defendant can locate the document providing his findings on the datasets, and the other datasets he was evaluating suffered from the same setbacks as the DiF Dataset. *Id*. at 139:4-19; 254:16-255:17; 345:19-346:7; 326:5-23; Ex. 15 (May 11, 2022 Email). Without knowing which datasets were used to accomplish Mr. Skrainka's work, material questions of fact exists as to whether the DiF Dataset was used and whether Microsoft benefited.

CONCLUSION

Accordingly, the Court should deny Defendant's motion for summary judgment.

---

prior findings to maintain consistency and avoid reconsideration of matters once decided, during the course of a single continuing lawsuit. These are the goals this doctrine is meant to further. *See Ingle v. Circuit City*, 408 F.3d 592, 594 (9th Cir. 2005).

DATED: July 1, 2022

By: *s/ Nicholas R. Lange*
Katrina Carroll, Admitted *pro hac vice*
Nicholas R. Lange, Admitted *pro hac vice*
LYNCH CARPENTER LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
Telephone: (312) 750-1265
Email: katrina@lcllp.com
Email: nickl@lcllp.com

Gary Lynch, Admitted *pro hac vice*
Kenneth Held, Admitted *pro hac vice*
LYNCH CARPENTER LLP
1133 Penn Avenue, Floor 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Email: gary@lcllp.com
Email: ken@lcllp.com

David B. Owens, WSBA #52856
LOEVY & LOEVY
100 S. King Street, Suite 100
Seattle, WA 98104
Telephone: (312) 243-5900
Fax: (312) 243-5092
Email: david@loevy.com

By: *s/ Scott R. Drury*
Scott R. Drury, Admitted *pro hac vice*
Mike Kanovitz, Admitted *pro hac vice*
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, IL 60607
Telephone: (312) 243-5900
Email: drury@loevy.com
Email: mike@loevy.com

Attorneys for Plaintiffs