UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

BRIAN STREIT, Ph.D.
5692 N Galena St
Denver, Colorado 80238

Plaintiff,

v.

PRIVATE IDENTITY LLC (f.k.a. OPEN INFERENCE HOLDINGS LLC)
A Delaware limited liability company,
13331 Signal Tree Lane
Potomac, Maryland 20854

Defendant.

Civil Action No. 8:23-cv-2031

COMPLAINT
Jury Demand

COMPLAINT

Plaintiff Brian Streit, Ph.D. ("Plaintiff" or "Dr. Streit") for his Complaint against PRIVATE IDENTITY LLC (f.k.a. OPEN INFERENCE HOLDINGS LLC), a Delaware limited liability company ("Defendant" or "PI"), alleges as follows.

NATURE OF THE ACTION

1. This is an action to correct inventorship under 35 U.S.C. § 256 with respect to fifteen United States patents: United States Patent No. 10,419,221 (the "'221 patent"); United States Patent No. 10,721,070 (the "'070 patent"); United States Patent No. 10,938,852 (the "'852 patent"); United States Patent No. 11,122,078 (the "'078 patent"); United States Patent No. 11,138,333 (the "'333 patent"); United States Patent No. 11,170,084 (the "'084 patent"); United States Patent No. 11,210,375 (the "'375 patent"); United States Patent No. 11,265,168 (the "'168 patent"); United States Patent No. 11,362,831 (the "'831 patent"); United States Patent No. 11,392,802 (the "'802 patent"); United States Patent No.

11,394,552 (the "'552 patent"); United States Patent No. 11,489,866 (the "'866 patent"); United States Patent No. 11,502,841 (the "'841 patent"); United States Patent No. 11,640,452 (the "'452 patent"); and United States Patent No. 11,677,559 (the "'559 patent") (collectively the "Patents"). Each of the Patents issued names only Scott Edward Streit ("Scott Streit") as an inventor, and each is assigned to Defendant. Copies of the Patents are attached hereto as Exhibits A through O, respectively.

2. This also is an action under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, and the Patent Act, 35 U.S.C. §§ 261 and 262, seeking a declaration that, as a joint inventor, Dr. Streit is a co-owner with Defendant of an undivided interest in each of the Patents.

3. The case concerns a pioneering development in the field of personal identity assurance and identity validation using biometric data that has been encrypted. More particularly, the Patents provide solutions that include comparing biometric data acquired from a given individual and encrypted in polynomial time to previously acquired and stored encrypted biometric data of many known individuals. The Patents address matching the acquired biometric data with the stored biometric data to validate the identity of the given individual. In specific instances, biometric data are acquired and applied in one way homomorphic encryption to produce Euclidean measurable feature vectors which are used to associate a label identifying the person as known. When an identity assurance or verification is to be conducted, the acquired biometric data can be converted into homomorphic encrypted Euclidean measurable feature vectors via a deep neural network in conjunction with another neural network, and a search for a match is conducted, which will return either a label identifying the person known based on a matching of acquired to a stored vector, or an "unknown" response in the absence of such a match. Importantly, patented solutions

work with different biometric data, including a person's face, voice, fingerprints, iris, retina, health data (EEG), etc. The patented solutions provide a number of advantages in improved security, e.g., the acquired biometric data that might be linked to an individual is not retained; no decryption key is needed to process the homomorphic encrypted data, and improved processing speed and reduced processing power, memory and time, which enables use of the solution on conventional mobile devices.

4. Dr. Streit's contributions to the inventions set forth in at least the Patents in Exhibits A through O, including his conception, development, and implementations which are described and claimed therein, occurred over at least the period of time from 2017 through 2018. Dr. Streit's inventive contributions were shared and documented in extensive interactions between he and the named inventor on the patents, Scott Streit. In addition, Dr. Streit worked with Mr. Nguyen Chung, an outside contractor who provided various technical support services as Scott Streit and Dr. Streit invented the solutions described and claimed in the Patents in Exhibits A through O.

5. Dr. Streit's inventive contributions made during this period from at least 2017 through 2018 are well-documented in written email, texts, meeting notes, and programming code including as respectively between Dr. Streit, Scott Streit, Nguyen Chung, and Michael Pollard of OPEN INFERENCE HOLDINGS LLC.

6. At least during the period between 2017 and 2018, Dr. Streit worked continuously with Scott Streit while developing the solutions described and claimed in the Patents in Exhibits A through O.

PARTIES

7. Plaintiff resides in Denver, Colorado.

8. Defendant is a Delaware Limited Liability Company with its principal place of business located at 13331 Signal Tree Lane, Potomac, Maryland 20854. On information and belief, Defendant has two members, Michael Pollard who resides in Maryland, and Scott Streit who resides in Maryland.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331, 1338 and 35 U.S.C. §§ 256, 261, and 262 and 28 U.S.C. §§ 2201 and 2202 (the "Declaratory Judgment Act").

10. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b), (c).

11. This Court has personal jurisdiction over Defendant to adjudicate this action for correction of inventorship under 35 U.S.C. § 256.

STATEMENT OF FACTS

I. The Collaboration Between Dr. Streit and Scott Streit

12. Throughout the period from at least January 2017 through March 2018, Dr. Streit and Scott Streit collaborated on inventions described and claimed in the Patents in Exhibits A through O, and Dr. Streit conceived of, developed, and implemented inventive features which are described and claimed therein.

13. For example, and without limitation, Dr. Streit jointly invented claimed features including "accept[ing] as an input encrypted feature vectors that are Euclidean measurable and are produced as a one way encoding of unencrypted biometric information by a first pre-trained neural network, and return[ing] an unknown result or a label as output during prediction" (US Application Serial No. 15/914,969, now US Patent No. 11,138,333).

14. Further, Dr. Streit jointly invented claimed features including "accept[ing] as an input feature vectors that are Euclidean measurable and return[ing] the unknown result or the label as output; wherein instantiating the classification component includes an act of allocating within at least one layer of the classification network, an initial number of classes and having a subset of the class slots that are unassigned" (US Application Serial No. 15/914,942, now US Patent No. 10,721,070).

15. Still further, Dr. Streit jointly invented claimed features including "training [a deep neural network ('DNN')] with [a] Euclidean measurable encrypted feature vector and label inputs, the act of training including defining the DNN for subsequent prediction operations executed responsive to input of an unknown Euclidean measurable encrypted feature vector" (US Patent Application Serial No. 15/914,436, now US Patent No. 10,419,221).

16. Moreover, Dr. Streit jointly invented claimed features including using "a classification network comprising a fully connected neural network ("FCNN") as a first member of a linked pair of networks and a feature vector generation component comprising a pre-trained convolutional neural network ("CNN") as a second member of the linked pair of networks [to generate] a first set of one-way encrypted Euclidean measurable feature vectors as an output of at least one layer in the pre-trained convolutional neural network ("CNN") responsive to input of an unencrypted biometric input to the pre-trained CNN" (US Application Serial No. 15/914,562, now US Patent No. 11,392,802). These patents were filed in 2018 during the period of collaboration between Dr. Streit and Scott Streit. All of the other patents in Exhibits A through O claim priority and incorporate by reference the four patents identified above and claim subject matter in which Dr. Streit made inventive contributions.

17. Also during this collaborative period, Dr. Streit co-authored a paper with Scott Streit, entitled "Privacy-Enabled Biometric Search," which is cited in the above-identified US patents, and includes material that represents Dr. Streit's collaboration and involvement in the technology described in the Patents in Exhibits A through O.

18. Evidence of Dr. Streit's collaboration and inventive contribution is well-documented and can be corroborated by individuals working with or on behalf of the Defendant during the period between 2017 and 2018. For example, text messages and e-mail communications by and between Dr. Streit, Scott Streit and Nugyen Chung, and between Scott Streit and Michael Pollard, corroborate Dr. Streit's involvement and inventive contributions. Dr. Streit's contributions can be further corroborated by Stephen Suffian and Nguyen Chung.

19. Accordingly, Dr. Streit is an unnamed, joint inventor on the Patents in Exhibits A through O. Dr. Streit was never employed by the Defendant, was not paid by the Defendant, and had no obligation to assign rights in any of his inventions, including those described and claimed in the Patents in Exhibits A through O. As such, Dr. Streit owns an undivided ownership interest in the Patents in Exhibits A through O.

II. The Patents

20. On March 7, 2018, Defendant filed four U.S. patent applications in the United States Patent and Trademark Office ("USPTO"), including U.S. Patent Application Serial Nos. 15/914,969, 15/914,942, 15/914,436, and 15/914,562. Each of the four patent applications identify Scott Streit as the only inventor. The four applications were prosecuted to allowance, and respectively issued as U.S. Patents. Specifically, the '333 patent issued on October 5, 2021 and is entitled "Systems and Methods for Privacy-Enabled Biometric Processing," the '070 patent issued on July 21, 2020 and is entitled "Systems and Methods for Privacy-Enabled Biometric Processing," the '221 patent issued on September 17, 2019

and is entitled "Systems and Methods for Privacy-Enabled Biometric Processing," and the '802 patent issued on July 19, 2022 and is entitled "Systems and Methods for Privacy-Enabled Biometric Processing." Significantly Dr. Streit is not named as a joint inventor on any of the '333, '070, '221, and '802 patents.

21. Claim 1 of the '333 patent is representative, and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, comprising a classification network having a deep neural network configured to:

classify Euclidean measurable encrypted feature vectors and label inputs for identification during training, and

accept as an input, to the deep neural network, encrypted feature vectors that are Euclidean measurable and are produced as a one way encoding of unencrypted biometric information by a first pre-trained neural network, and return an unknown result or a matching label as output; and

an enrollment interface configured to:

accept unencrypted biometric information;

provide Euclidean measurable encrypted feature vectors generated from the first pre-trained neural network based on the unencrypted biometric information;

delete the unencrypted biometric information responsive to generation of the Euclidean measurable encrypted feature vectors by the first pre-trained neural network;

provide a respective label to the classification component for training; and

trigger the classification component to train the deep neural network on the Euclidean

measurable encrypted feature vectors to link the label to respective encrypted feature vectors;

wherein the first pre-trained neural network is configured to:

accept unencrypted biometric information; and

encode the unencrypted biometric information into Euclidean measurable encrypted feature vectors as one way encodings of the unencrypted biometric information."

22. Claim 1 of the '979 patent is representative, and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, including a classification network having a deep neural network ("DNN") configured to classify feature vector and label inputs during training and return a label for person identification or an unknown result during prediction, wherein the classification component is further configured to accept as an input feature vectors that are Euclidean measurable;

the classification network having an architecture comprising a plurality of layers: at least one layer comprising nodes associated with feature vectors, the at least one layer having an initial number of identification nodes and a subset of the identification nodes that are unassigned;

wherein the system responsive to input of biometric information for a new user is configured to trigger an incremental training operation for the classification network integrating the new biometric information into a respective one of the unallocated identification nodes usable for subsequent matching."

23. Claim 1 of the '221 patent is representative, and recites: "A privacy-enabled biometric

system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, comprising a classification network having a deep neural network ("DNN"), the DNN configured to:

classify Euclidean measurable encrypted feature vector and label inputs during training, wherein training of the DNN is executed on the Euclidean measurable encrypted feature vector inputs to the DNN, the training defining the DNN for subsequent prediction operations on input of an unknown encrypted feature vector to the DNN; and

return a label for person identification or an unknown result during prediction, and

wherein the DNN is further configured to:

accept as an input at least one unclassified encrypted feature vector that is Euclidean measurable to the DNN during prediction;

generate an array of values in response to the input of the at least one unclassified encrypted feature vector during prediction;

determine a label or unknown result based on analyzing a position of values within the array and analyzing a respective value at a respective position; and

wherein the classification component is further configured to return the unknown result if there is no associated label and the label as output if there is an associated label responsive to the analyzing of the position of values within the array and the analyzing of the respective value at the respective position."

24. Claim 1 of the '802 patent is representative, and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, including at least one classification network having a fully connected neural network ("FCNN") that is a first member of at least one linked pair of neural networks, the FCNN configured to:

classify a first set of one-way Euclidean measurable encrypted feature vectors generated by a second member of the at least one linked pair of neural networks and respective label inputs during training;

define at least a plurality of identification classes, each corresponding to an identity and respective label associated with the identity for subsequent identification;

return a label associated with a respective identification class for person identification responsive to matching to the respective identification class and an unknown result responsive to failing to match to the plurality of identification classes during prediction, responsive to input of a newly generated one-way encrypted Euclidean measurable feature vector;

a feature vector generation component comprising at least a pre-trained convolutional neural network ("CNN") as the second member of the at least one linked pair of neural networks, the pre-trained CNN configured to generate the first set of the one-way encrypted Euclidean measurable feature vectors used by the FCNN as an output of a least one layer in the pre-trained CNN responsive to input of an unencrypted biometric input to the pre-trained CNN, the unencrypted biometric input captured on and identifying a subject for identification or authentication, wherein the at least one linked pair of networks are linked based on a biometric data type; and

wherein the classification component further comprises a second classification network

that is a first member of a second linked pair of networks, the second classification network is configured to accept one-way encrypted feature vectors from a second pre-trained neural network that is a second member of the second linked pair of networks that generates a second set of one-way encrypted feature vectors on a second biometric type."

25. On June 28, 2018, Defendant filed U.S. patent application No. 16/022,101, which was prosecuted and subsequently issued on November 9, 2021 as the '084 patent entitled "Biometric Authentication."

26. Claim 1 of the '084 patent is representative, and recites: "A method of authorizing access to access-controlled environments, the method comprising:

receiving, passively by a computing device, user behavior authentication information indicative of a behavior of a user of the computing device;

comparing, by the computing device, the user behavior authentication information to a stored user identifier associated with the user;

calculating, by the computing device, a user identity probability based on a plurality of authentication sources, wherein the act of calculating includes:

determining a first portion of the user identity probability based on the comparison of the user behavior authentication information to the stored user identifier as a first source,

determining a second portion of the user identity probability based on active authentication input by the user as a second source; and

determining a third portion of the user identity probability based on a liveness evaluation as a third source, wherein the liveness evaluation is based on authentication information that validates capture of the first and second source of authentication information by a

live user;

receiving, by the computing device, a request from the user to execute an access-controlled function;

granting, by the computing device, the request from the user responsive to determining that the user identity probability satisfies a first identity probability threshold associated with the access-controlled function; and

wherein the determining the third portion of the user identity probability based on the liveness evaluation includes an act of processing the authentication information that validates the capture of the first and second source using at least one neural network, wherein the at least one neural network is configured to accept the authentication information as an input, generate an output probability that the user behavior authentication information and the active authentication information input are actually obtained from the user, and wherein determining the third portion of the user identity probability is based, at least in part, on the output probability."

27. On August 14, 2020, Defendant filed U.S. patent application No. 16/903,596 which was prosecuted and subsequently issued on March 2, 2021 as the '852 patent entitled "Systems and Methods for Private Authentication With Helper Networks."

28. Claim 1 of the '852 patent is representative, and recites: "An authentication system for privacy-enabled authentication, the system comprising:

at least one processor operatively connected to a memory;

an authentication data gateway, executed by the at least one processor, configured to filter invalid identification information, the authentication data gateway comprising at least:

a first pre-trained geometry helper network, wherein the first pre-trained geometry helper

network is trained on a plurality of identification samples of a first type to filter identifying characteristics from input identification information of the first type, and configured to:

process the input identification information of the first type,

accept as input plaintext identification information of the first type, and

output the processed input identification information of the first type, wherein the processed input identification information of the first type includes the filtered identifying characteristics from the input identification information of the first type; and

a first pre-trained validation helper network trained on a plurality of valid and invalid samples of the first type, the first pre-trained validation helper network associated with the first pre-trained geometry helper network, and configured to:

process the input identification information of the first type,

accept the output of the first pre-trained geometry helper neural network, and

validate the input identification information of the first type or reject the input identification information of the first type,

wherein the geometry and validation helper networks process the input identification information and output filtered identification information used for subsequent enrollment and identification functions; and

wherein the authentication data gateway further comprises a plurality of validation helper networks each associated with a respective type of identification information, wherein each of the plurality of validation helper networks generate at least a binary evaluation of respective identification inputs to establish validity."

29. On February 24, 2021, Defendant filed U.S. patent application No. 17/183,950, as a continuation of application No. 16/993,596 filed on August 14, 2020, which was prosecuted and subsequently issued on September 14, 2021 as the '078 patent entitled "Systems and Methods for Private Authentication With Helper Networks."

30. Claim 1 of the '078 patent is representative, and recites: "An authentication system for privacy-enabled authentication, the system comprising:

at least one processor operatively connected to a memory;

an authentication data gateway, executed by the at least one processor, configured to filter identification information used in enrollment, identification, or authentication functions of subsequent neural networks, the authentication data gateway comprising at least:

a first pre-trained validation helper network associated with identification information of a first type comprising voice identification information, wherein the first pre-trained validation helper network is configured to:

evaluate an unknown identification sample of the first type, responsive to input of the unknown information sample of the first type to the first pre-trained validation helper network, wherein the first pre-trained validation helper network is pre-trained on evaluation criteria that is independent of a subject of the identification information seeking to be enrolled, identified, or authenticated;

responsive to a determination that the unknown identification sample meets the evaluation criteria, validate the unknown information sample for use in subsequent enrollment, identification, or authentication;

responsive to a determination that the unknown identification sample fails the evaluation

criteria, reject the unknown information sample for use in subsequent enrollment, identification, or authentication; and

generate at least a binary evaluation of the unknown identification information sample based on the determination of the evaluation criteria, wherein the at least the binary evaluation includes generation of an output probability by the first pre-trained validation helper network that the unknown identification information sample is valid or invalid."

31. On December 12, 2018, Defendant filed U.S. patent application No. 16/218,139 as a continuation-in-part of application No. 15/914,562 filed on March 7, 2018 and a continuation in part of application No.15/914,942 and a continuation in part of application No. 15/914,969 filed on March 7, 2018, which was prosecuted and subsequently issued on December 28, 2021 as the '375 patent entitled "Systems and Methods for Biometric Processing With Liveness."

32. Claim 1 of the '375 patent is representative, and recites: "An authentication system for evaluating privacy-enabled biometrics and validating contemporaneous input of biometrics, the system comprising:

at least one processor operatively connected to a memory;

an interface, executed by the at least one processor configured to:

receive a candidate set of instances of a first biometric data type input by a user requesting authentication;

a classification component executed by the at least one processor, configured to:

analyze a liveness threshold, wherein analyzing the liveness threshold includes processing the candidate set of instances to determine that the candidate set of instances matches

a random set of instances;

the classification component further comprising at least a first deep neural network ("DNN"), the classification component configured to:

accept, as an input to the first DNN, one-way homomorphic encrypted feature vectors, output from at least one layer of a first neural network, the first neural network configured to process a plaintext input of the first biometric data type into the one-way homomorphic encrypted feature vectors;

classify, with the first DNN during training, the one-way homomorphic encrypted feature vectors of the first biometric data type, based on training the first DNN with the one-way homomorphic encrypted feature vectors and respective labels taken as inputs;

define at least a plurality of identification classes during training of the first DNN, wherein respective identification classes correspond to the respective labels, and the respective labels are associated with respective user identities;

return, during prediction, a matching label for person identification from the plurality of identification classes in response to a match and an unknown result responsive to failure to match to the plurality of identification classes based, at least in part, on analyzing one-way homomorphic encrypted feature vectors with the first DNN; and

confirm the matching label based at least on the liveness threshold."

33. On August 13, 2019, Defendant filed U.S. patent application No. 16/539,824 as a continuation in part of application No. 16/218,139 filed on December 12, 2018, which was filed on March 7, 2018, and a continuation in part of application No. 15/914,942, filed on March 7, 2018, and a continuation in part of application No. 15/914,969, filed on March 7, 2018, and application No. 16/539,824, and a continuation in part of application No.

15/914,436 filed on March 7, 2018, and a continuation in part of application No. 15/914,562, filed on March 7, 2018, and a continuation in part of application No. 15/914,942, filed on March 7, 2018, and a continuation in part of application No. 15/914,969 filed on March 7, 2018, which was prosecuted and subsequently issued on March 1, 2022 as the '168 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

34. Claim 1 of the '168 patent is representative, and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory, the at least one processor configured to:

determine an authentication mode;

trigger one or both of a first machine learning ("ML") process or a second ML process responsive to determining the authentication mode;

execute the first ML process, wherein the first ML process when executed by the at least one processor is configured to:

accept distance measurable encrypted feature vector and label inputs during training of a first classification neural network and classify distance measurable encrypted feature vector inputs as part of authentication using the first classification network once trained;

execute the second ML process, wherein the second ML process when executed by the at least one processor is configured to:

accept plain text biometric inputs during training of a generation neural network to generate distance measurable encrypted feature vectors; and

compare distances between distance measurable encrypted feature vectors during

authentication."

35. On July 20, 2020, Defendant filed U.S. patent application No. 16/933,428 as a continuation of application No. 15/914,942, filed on March 7, 2018, which was prosecuted and subsequently issued on June 14, 2022 as the '831 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

36. Claim 1 of the '831 patent is representative, and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, including a classification network having a deep neural network ("DNN"), the DNN configured to:

accept as an input distance measurable encrypted feature vectors, the distance measurable encrypted feature vectors generated as a one way encoding of plain text authentication information input to at least one first neural network;

train, the DNN, on distance measurable encrypted feature vector and respective label inputs; and

predict a match to a label for identification or return unknown responsive to input of at least one distance measurable encrypted feature vector produced by the at least one first neural network."

37. On March 27, 2020, Defendant filed U.S. patent application No. 16/832,014 as a continuation in part of application No. 16/573,851 filed on September 17, 2018, which is a continuation in part of application No. 16/539,824, filed on August 13 , 2019, which is a continuation in part of application No.16/218,139 filed on December 12, 2018, which was filed on March 7, 2018, and a continuation in part of application No. 15/914,942, filed on

March 7, 2018, and a continuation in part of application No. 15/914,969, filed on March 7, 2018, and application No. 16/539,824, and a continuation in part of application No. 15/914,436 filed on March 7, 2018, and a continuation in part of application No. 15/914,562, filed on March 7, 2018, and a continuation in part of application No. 15/914,436, filed on March 7, 2018, which was prosecuted and subsequently issued on July 19, 2022 as the '552 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

38. Claim 1 of the '552 patent is representative, and recites: "An authentication system for privacy-enabled authentication, the system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, comprising at least a first deep neural network ("DNN"), the first DNN configured to:

accept encrypted authentication credentials, generated from a first neural network as input to the first DNN;

classify the encrypted authentication credentials during training, based on processing the encrypted authentication credentials and associated label inputs during the training;

output an array of values, from the first DNN, reflecting a probability of a first match to at least one label of the associated label inputs for identification responsive to analyzing at least one of the encrypted authentication credentials input during prediction; and

wherein the classification component is further configured to:

retrieve at least one of the encrypted authentication credentials classified during training from the memory based on identification in the array of values establishing the first match to an identity;

determine a distance between the at least one of the encrypted authentication credentials input during prediction and the at least one encrypted authentication credential retrieved; and

return a distance match, responsive to determining the distance between the encrypted authentication credential input and the at least one encrypted authentication credential meets a threshold for validating a second match to the identity."

39. On August 10, 2021, Defendant filed U.S. patent application No. 17/398,555 as a continuation in part of application No. 17/183,950 filed on February 24, 2021, and a continuation in part of application No. 16/993,596 filed on August 14, 2020, and a continuation in part of application No. 16/832,014 as a continuation in part of application No. 16/573,851 filed on September 17, 2018, which is a continuation in part of application No. 16/539,824, filed on August 13, 2019, which is a continuation in part of application No. 16/218,139 filed on December 12, 2018, which was filed on March 7, 2018, which is a continuation in part of application No. 16/022,101 filed on June 28, 2018, and a continuation in part of application No. 15/914,942, filed on March 7, 2018, and a continuation in part of application No. 15/914,969, filed on March 7, 2018, and application No. 16/539,824, and a continuation in part of application No. 15/914,436 filed on March 7, 2018, and a continuation in part of application No. 15/914,562, filed on March 7, 2018, and a continuation in part of application No. 15/914,436, filed on March 7, 2018, which was prosecuted and subsequently issued on November 1, 2022 as the '866 patent entitled "Systems and Methods for Private Authentication With Helper Networks."

40. Claim 1 of the '866 patent is representative, and recites: "A system for managing privacy-enabled identification or authentication, the system comprising:

at least one processor operatively connected to a memory;

an identification data gateway, executed by the at least one processor, configured to filter invalid identification information from subsequent verification, enrollment, identification, or authentication functions, the identification data gateway comprising at least:

a first pre-trained validation helper network associated with identification information of a first type, wherein the first pre-trained validation helper network comprises a pre-trained neural network configured to:

evaluate an identification instance of the first type captured on a subject to determine if the identification instance is suitable for use, responsive to input of the identification instance of the first type to the first pre-trained validation helper network, wherein the first pre-trained validation helper network is pre-trained on evaluation criteria that is independent of identification of the subject of the identification instance seeking to be enrolled, identified, or authenticated:

responsive to a determination that the identification instance meets the evaluation criteria, validate the identification instance for use in subsequent verification, enrollment, identification, or authentication that establish the identity of the subject;

responsive to a determination that the identification instance fails the evaluation criteria, reject the information instance for use in subsequent verification, enrollment, identification, or authentication that establish the identity of the subject; and

generate at least a binary evaluation of the identification information instance based on the determination of the evaluation criteria, wherein the at least the binary evaluation includes generation of an output probability by the first pre-trained validation helper

network that the identification instance is a valid or an invalid identification information instance;

wherein the authentication data gateway further comprises a plurality of validation helper networks associated with a respective type of identification information including the first pre-trained validation helper network, wherein the plurality of validation helper networks generate at least a binary evaluation of respective identification information inputs, and are configured to validate respective identification information independent of the subject seeking to be enrolled, identified, or authenticated; and include

a first voice helper network trained to validate respective voice identification information independent of the subject seeking to be enrolled, identified, or authenticated; and

a first image helper network trained to validate respective image identification information independent of the subject seeking to be enrolled, identified, or authenticated."

41. On September 17, 2019, Defendant filed U.S. patent application No. 17/573,851 as a continuation in part of application No. 16/539,824 filed August 13, 2019, and a continuation in part of application No. 16/218,139 filed on December 12, 2018, which was filed on March 7, 2018, and a continuation in part of application No. 15/914,942, filed on March 7, 2018, and a continuation in part of application No. 15/914,969, filed on March 7, 2018, and application No. 16/539,824, and a continuation in part of application No. 15/914,436 filed on March 7, 2018, and a continuation in part of application No. 15/914,562, filed on March 7, 2018, and a continuation in part of application No. 15/914,942, filed on March 7, 2018, and a continuation in part of application No. 15/914,969 filed on March 7, 2018, which was prosecuted and subsequently issued on November 15, 2022 as the '841 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

42. Claim 1 of the '841 patent is representative, and recites: "A privacy-enabled authentication system comprising:

at least one processor operatively connected to a memory, the at least one processor configured to:

execute a first machine learning ("ML") and a second ML process responsive to an authentication mode;

determine the authentication mode;

trigger one or both of the first ML process or the second ML process responsive to determining the authentication mode;

wherein the first ML process when executed by the at least one processor is configured to:

accept distance measurable encrypted feature vector and label inputs during training of one or more first classification neural networks to define a plurality of identification classes and classify distance measurable encrypted feature vector inputs as part of authentication using the one or more first classification neural networks once trained;

wherein the second ML process when executed by the at least one processor is configured to:

accept plain text biometric or behavioral inputs as input to one or more generation neural networks and output respective distance measurable encrypted feature vectors;

compare distances between distance measurable encrypted feature vectors generated by respective neural networks during authentication; and

validate identification results produced by the first and second ML processes are captured from a live submission, the validation including operations to determine liveness in multiple dimensions including at least liveness evaluation of authentication inputs of a

matching type submitted to the first or second ML process, as part of the evaluation of the multiple dimensions."

43. On October 4, 2021, Defendant filed U.S. patent application No. 17/492,775 as a continuation of application No. 15/914,969 filed March 7, 2018, which was prosecuted and subsequently issued on May 2, 2023 as the '452 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

44. Claim 1 of the '452 patent is representative and recites: "A privacy-enabled biometric system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, comprising a classification network having a deep neural network, the deep neural network configured to:

classify distance measurable encrypted feature vectors and label inputs for identification during training,

accept as an input, to the deep neural network, encrypted feature vectors that are distance measurable and are produced as a one way encoding of plaintext biometric information by a first pre-trained neural network, and

predict an outcome based on a trained model and a set of inputs for the prediction to match to a result label or unknown;

return an unknown result or a matching label from a plurality of trained identification classes as an output of prediction; and

an enrollment interface configured to:

accept plaintext biometric information;

provide distance measurable encrypted feature vectors for classification generated from the first pre-trained neural network from the plaintext biometric information;

delete the plaintext biometric information responsive to generation of the distance measurable encrypted feature vectors by the first pre-trained neural network;

provide a respective label to the classification component for training with associated one or more distance measurable encrypted feature vectors; and

trigger the classification component to train the deep neural network on the distance measurable encrypted feature vectors to link the label to the associated encrypted feature vectors."

45. On June 13, 2022, Defendant filed U.S. patent application No. 17/838,643 as a continuation of application No. 16/933,428 filed on July 20, 2020, and a continuation of application No. 15/914,942, filed on March 7, 2018, which was prosecuted and subsequently issued on June 13, 2023 as the '559 patent entitled "Systems and Methods for Privacy-Enabled Biometric Processing."

46. Claim 1 of the '559 patent is representative, and recites: "A privacy-enabled identification system comprising:

at least one processor operatively connected to a memory;

a classification component executed by the at least one processor, including a classification model including one or more deep neural networks ("DNNs"), the one or more DNNs trained on distance measurable homomorphic encrypted feature vector and respective label inputs, and wherein the DNN is configured to:

accept as an input distance measurable homomorphic encrypted feature vectors, the distance measurable homomorphic encrypted feature vectors generated as a one way

encoding of plain text identification information of a first identification data type for an entity input to at least one first pre-trained neural network; and

predict a match to a label for identification or return unknown responsive to input of at least one distance measurable homomorphic encrypted feature vector produced by the at least one first neural network from identification information of the first identification data type."

47. In his calls, emails, texts, and other communications with Scott Streit, Dr. Streit did more than merely provide Scott Streit with well-known principles or explain the state of the art.

48. As part of his collaborative research with Scott Streit, Dr. Streit contributed his ideas to the total inventive concept that is claimed in each of the Patents.

49. Dr. Streit conceived and made significant contributions to important aspects and features of the inventions claimed in the Patents.

50. Dr. Streit is a joint inventor of each of the Patents.

51. As a joint inventor with no valid contractual obligation to assign his invention rights to another, Dr. Streit is a co-owner of each of the Patents.

COUNT I
(Correction of Inventorship of United States Patent No. 10,419,221)

52. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

53. Dr. Streit made significant contributions to the conception of the subject matter claimed in the '221 patent.

54. Dr. Streit and Scott Streit are joint inventors of the '221 patent.

COUNT II
(Correction of Inventorship of United States Patent No. 10,721,070)

55. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs

of this Complaint as if fully set forth herein.

56. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘070 patent.

57. Dr. Streit and Scott Streit are joint inventors of the ‘070 patent.

COUNT III
(Correction of Inventorship of United States Patent No. 10,938,852)

58. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

59. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘852 patent.

60. Dr. Streit and Scott Streit are joint inventors of the ‘852 patent.

COUNT IV
(Correction of Inventorship of United States Patent No.11,122,078)

61. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

62. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘078 patent.

63. Dr. Streit and Scott Streit are joint inventors of the ‘078 patent.

COUNT V
(Correction of Inventorship of United States Patent No. 11,138,333)

64. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

65. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘333 patent.

66. Dr. Streit and Scott Streit are joint inventors of the ’333 patent.

COUNT VI
(Correction of Inventorship of United States Patent No. 11,170,084)

67. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

68. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘084 patent.

69. Dr. Streit and Scott Streit are joint inventors of the ‘084 patent.

COUNT VII
(Correction of Inventorship of United States Patent No. 11,210,375)

70. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

71. Dr. Streit made significant contributions to the conception of the subject matter claimed in the’375 patent.

72. Dr. Streit and Scott Streit are joint inventors of the ‘375 patent.

COUNT VIII
(Correction of Inventorship of United States Patent No. 11,265,168)

73. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

74. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘168 patent.

75. Dr. Streit and Scott Streit are joint inventors of the ‘168 patent.

COUNT IX
(Correction of Inventorship of United States Patent No. 11,362,831)

76. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs

of this Complaint as if fully set forth herein.

77. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ’831 patent.

78. Dr. Streit and Scott Streit are joint inventors of the ‘831 patent.

COUNT X
(Correction of Inventorship of United States Patent No. 11,392,802)

79. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

80. Dr. Streit made significant contributions to the conception of the subject matter claimed in the’802 patent.

81. Dr. Streit and Scott Streit are joint inventors of the ‘802 patent.

COUNT XI
(Correction of Inventorship of United States Patent No. 11,394,552)

82. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

83. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘552 patent.

84. Dr. Streit and Scott Streit are joint inventors of the ‘552 patent.

COUNT XII
(Correction of Inventorship of United States Patent No. 11,489,866)

85. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

86. Dr. Streit made significant contributions to the conception of the subject matter claimed in the ‘866 patent.

87. Dr. Streit and Scott Streit are joint inventors of the ‘866 patent.

COUNT XIII
(Correction of Inventorship of United States Patent No. 11,502,841)

88. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

89. Dr. Streit made significant contributions to the conception of the subject matter claimed in the '841 patent.

90. Dr. Streit and Scott Streit are joint inventors of the '841 patent.

COUNT XIV
(Correction of Inventorship of United States Patent No. 11,640,452)

91. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

92. Dr. Streit made significant contributions to the conception of the subject matter claimed in the '452 patent.

93. Dr. Streit and Scott Streit are joint inventors of the '452 patent.

COUNT XV
(Correction of Inventorship of United States Patent No. 11,677,559)

94. Plaintiff repeats and realleges the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

95. Dr. Streit made significant contributions to the conception of the subject matter claimed in the '559 patent.

96. Dr. Streit and Scott Streit are joint inventors of the '559 patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

A. An Order determining and declaring that Plaintiff Brian Streit is a joint inventor of the Patents.

B. An Order directing the United States Patent and Trademark Office to correct inventorship of the Patents by adding Brian Streit as a joint inventor.

C. An Order determining that this is an exceptional case under 35 U.S.C. § 285 and awarding Dr. Streit his reasonable attorney fees and costs; and

D. Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial on all issues so triable by jury.

Dated: July 27, 2023

Respectfully submitted,

*/s/*_____

Adam D. Greivell, Esq.
Md. Bar No. 28917
Greivell & Garrott Johnson, LLC
5 Cornell Avenue
Hagerstown, Maryland 21742
Telephone (240) 310-9150
adam@greivelllawoffice.com

Robert M. Isackson (to be admitted *pro hac vice*)
Leason Ellis LLP
One Barker Avenue, Fifth Floor
White Plains, NY 10601
Tel: (914) 288-0022
isackson@leasonellis.com;
lelitdocketing@leasonellis.com

Attorneys for Plaintiff Brian Streit, Ph.D.