

**COPY**

**FILE BY FAX**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Eric H. Gibbs (State Bar No. 178658)  
Andre M. Mura (State Bar No. 298541)  
Amanda M. Karl (State Bar No. 301088)  
Jeffrey B. Kosbie (State Bar No. 305424)  
**GIBBS LAW GROUP LLP**  
505 14th Street, Suite 1110  
Oakland, California 94612  
Telephone: (510) 350-9700  
Fax: (510) 350-9701  
*ehg@classlawgroup.com*  
*amm@classlawgroup.com*  
*amk@classlawgroup.com*  
*jbk@classlawgroup.com*

Jennifer D. Bennett (State Bar No. 296726)  
Neil K. Sawhney (State Bar No. 300130)  
**GUPTA WESSLER PLLC**  
100 Pine Street, Suite 1250  
San Francisco, CA 94111  
(415) 573-0336  
*jennifer@guptawessler.com*  
*neil@guptawessler.com*

Benjamin Elga (pro hac vice forthcoming)  
Alice Buttrick (pro hac vice forthcoming)  
**JUSTICE CATALYST LAW INC.**  
81 Prospect St., 7th Floor  
Brooklyn, NY 11201  
(518) 732-6703  
*belga@justicecatalyst.org*  
*abuttrick@justicecatalyst.org*

*Attorneys for Plaintiffs*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
COUNTY OF ALAMEDA**

CAT BROOKS and RASHEED  
SHABAZZ, individually and on behalf  
of all others similarly situated,  
  
Plaintiffs,  
  
v.  
  
THOMSON REUTERS CORPORATION,  
  
Defendant.

Albert Fox Cahn (pro hac vice forthcoming)  
**SURVEILLANCE TECHNOLOGY  
OVERSIGHT PROJECT**  
40 Rector Street, 9th Floor  
New York, NY 10006  
*albert@stopspying.org*

**ENDORSED  
FILED  
ALAMEDA COUNTY  
DEC 03 2020  
CLERK OF THE SUPERIOR COURT  
By TANIA PIERCE  
TANIA PIERCE Deputy**

Case No. Rg20082878  
**CLASS ACTION COMPLAINT  
DEMAND FOR JURY TRIAL  
COMPLEX**

**CLASS ACTION COMPLAINT**

1           1. Thomson Reuters is best known for its news agency (Reuters) and its online legal-  
2 research service (Westlaw). But the company makes money in another, lesser-known way: It  
3 collects a vast quantity of photos, identifying information, and personal data from American  
4 consumers, including Californians, without their consent and sells that information to  
5 corporations, law enforcement, and government agencies. Those whose identities the company  
6 sells, however, receive no compensation. Most of them don't even know it is happening.

7           2. Thomson Reuters sells this information through an online platform it calls CLEAR.  
8 CLEAR provides access to a database that aggregates both public and non-public information  
9 about millions of people and contains detailed cradle-to-grave dossiers on each person,  
10 including names, photographs, criminal history, relatives, associates, financial information,  
11 and employment information. The company advertises that CLEAR enables its users to access  
12 "both surface and deep web data to examine intelligence" about people "not found in public  
13 records or traditional search engines." This allows CLEAR users "to uncover" personal "facts  
14 hidden online," by scraping "real-time information" about individuals from social networks,  
15 blogs, and even chat rooms. The CLEAR database also includes information from third-party  
16 data brokers and law enforcement agencies that are not available to the general public,  
17 including live cell phone records, location data from billions of license plate detections, real-  
18 time booking information from thousands of facilities, and millions of historical arrest records  
19 and intake photos. This information is "fused and vetted by algorithm to form" what the *New*  
20 *York Times* described as "an ever-evolving, 360-degree view of U.S. residents' lives."<sup>1</sup>

21           3. Because of CLEAR, Californians' identities are up for sale without their knowledge,  
22 let alone consent. Named plaintiff Cat Brooks, for example, is an activist, who has spent years  
23 fighting police violence, particularly in communities of color. Because of her work, Ms. Brooks  
24 is targeted by white supremacist groups. Concerned for her safety and that of her family, Ms.  
25 Brooks works hard to maintain ownership and control over her personal information. She even  
26 subscribes to a service that routinely scrubs her personal information from the internet. Yet,

27 \_\_\_\_\_  
28 <sup>1</sup> McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 3, 2019)  
<https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

1 CLEAR offers a “360-degree view” of her life: Her address, her cell phone number, and  
2 information about her relatives, neighbors, and associates, are all for sale without her consent.

3 4. Ms. Brooks is not alone. Thomson Reuters sells detailed dossiers on Californians  
4 across the state, people who have no idea their personal information is being appropriated,  
5 aggregated, and sold over the internet. California’s common law right of publicity has long  
6 protected the right of its residents to determine for themselves whether, how, and to what  
7 extent their personal information is disseminated. Similarly, California’s Unfair Competition  
8 Law prohibits corporations from engaging in unlawful and unfair acts, which include  
9 appropriating a person’s personal information and selling it without their consent. Yet that is  
10 precisely what Thomson Reuters is doing with CLEAR, depriving Californians of their  
11 autonomy, dignity, and ownership of their own identities in the process.

12 5. This lawsuit seeks to remedy Thomson Reuters’ repeated violations of the plaintiffs  
13 and class members’ publicity rights and to enjoin the company from continuing to profit off  
14 their personal information without their consent.

### 15 **PARTIES**

16 6. Plaintiff Cat Brooks is a resident of Alameda County, California, whose name,  
17 photo, likeness, and other personal information Thomson Reuters has appropriated and sold  
18 without her consent.

19 7. Plaintiff Rasheed Shabazz is a resident of Alameda County, California, whose name,  
20 photo, likeness, and other personal information Thomson Reuters has appropriated and sold  
21 without his consent.

22 8. Defendant Thomson Reuters Corporation is a multinational media company  
23 headquartered in Toronto, Canada.

### 24 **JURISDICTION AND VENUE**

25 9. This Court has jurisdiction over this matter because Thomson Reuters is licensed to  
26 do business in California, regularly conducts business in California, and purposefully targets  
27 California residents for the collection and sale of personal information without consent. The  
28

1 company also regularly collects information about California residents from California sources.  
2 And it systematically sells CLEAR to California residents.

3 10. Venue is appropriate in this Court under Code of Civil Procedure section 395(b)  
4 because Thomson Reuters does not reside in this state and Plaintiffs reside in Alameda County,  
5 California.

## 6 FACTUAL ALLEGATIONS

### 7 **CLEAR aggregates billions of data points about individuals and sells this information** 8 **without obtaining consent or providing compensation.**

9 11. Thomson Reuters collects and aggregates “billions of data points” about  
10 individuals—including their photos, names, and personal identifying information—into  
11 searchable dossiers about each person and sells these dossiers through its CLEAR platform for  
12 substantial profits.<sup>2</sup>

13 12. At no point during its process of collecting, packaging, and selling individual  
14 information does Thomson Reuters ever ask individuals for their consent. In the vast majority  
15 of cases, the individuals do not even know that Thomson Reuters has collected their personal  
16 information and data—let alone that it is selling this information for profit.

17 13. Thomson Reuters has never offered individuals compensation for the sale of their  
18 photos, names, identifying information, or other personal data. And it provides no mechanism  
19 by which individuals can seek compensation.

20 14. The information aggregated and stored on the CLEAR database—which the  
21 company collects from public records, government sources, internet searches, and third-party  
22 data brokers—is highly personal and even confidential. For example, the CLEAR database  
23 includes data from government agencies and corporations that is not available to the general  
24 public, such as live cell phone records and license plate detections.

25 15. Thomson Reuters also collects data from law enforcement, including real-time  
26 booking images and information from local jails and corrections departments. According to its

27 \_\_\_\_\_  
28 <sup>2</sup>Thomson Reuters, *Thomson Reuters CLEAR*,  
<https://legal.thomsonreuters.com/en/products/clear-investigation-software>.

1 website, Thomson Reuters has acquired 90 million historical arrest records, including intake  
2 photos. Taken together, Thomson Reuters estimates that CLEAR houses over 38 million images  
3 gathered from over 2,000 agencies in over 40 states.<sup>3</sup>

4 16. In addition, the company purchases and consolidates information held by third-  
5 party data tracking firms, data brokers, and other companies that compile consumer and  
6 location data – private firms that the *Wall Street Journal* once dubbed “Big Brother-in-Law.”<sup>4</sup>  
7 This information includes data from credit agencies, DMV records, cellphone registries, social-  
8 media posts, property records, utility accounts, professional and fishing licenses, internet chat  
9 rooms, court records, and bankruptcy filings. All of this information is then “fused and vetted  
10 by algorithm to form an ever-evolving, 360-degree view of U.S. residents’ lives.”<sup>5</sup>

11 17. Even with respect to public-record information, CLEAR gives users the ability to  
12 search and analyze massive amounts of data that they would not otherwise be able to access  
13 on their own – in almost real time. For example, CLEAR has “real-time access to address and  
14 name-change data from credit reports and to motor-vehicle registrations from 43 U.S. states  
15 plus the District of Columbia and Puerto Rico.” And its “utility records, which come from more  
16 than 80 electric, gas, water, telephone, cable and satellite television companies nationwide, are  
17 updated daily.” Likewise, “[i]ncarceration and arrest records, often paired with booking photos  
18 that allow for facial-recognition-powered virtual lineups, arrive almost immediately from 2,100  
19 state and local agencies.”<sup>6</sup>

20 18. On the page of its website describing CLEAR’s corporate pricing plans, Thomson  
21 Reuters explains that its “intermediate” and “comprehensive” plans permit users to access  
22 “both surface and deep web data,” which includes data that is not ascertainable via public  
23 records or traditional search engine queries.<sup>7</sup> A marketing brochure similarly states that

24 <sup>3</sup>Thomson Reuters, *CLEAR Plans and Pricing*,

25 <https://legal.thomsonreuters.com/en/products/clear-investigation-software/plans-pricing>.

26 <sup>4</sup> McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 3, 2019)

27 <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

28 <sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> Thomson Reuters CLEAR Plans and Pricing, <https://legal.thomsonreuters.com/en/products/clear-investigation-software/plans-pricing#corporate>.

1 CLEAR's "Web Analytics" are capable of uncovering "facts hidden online" through its deep  
2 web search technology.<sup>8</sup>

3 19. In addition, corporate customers who purchase CLEAR's "comprehensive" plan  
4 have access to not only individuals' own personal information, but computer-generated lists of  
5 that subject's relatives and associates and their personal information.<sup>9</sup>

6 **CLEAR sells customers the ability to easily and quickly search for a specific individual's**  
7 **personal and non-public information**

8 20. Thomson Reuters advertises CLEAR as a "user-friendly platform," which offers  
9 customers an "easier . . . search experience that brings together key proprietary and public  
10 records into one intuitive, customizable environment." According to the company, CLEAR  
11 allows users to "quickly search across thousands of data sets and get accurate results in less  
12 time."

13 21. CLEAR's products are widely used. The platform receives approximately 100,000  
14 search queries each day.

15 22. Users sign into the CLEAR platform through a portal similar to Thomson Reuters'  
16 well-known Westlaw sign-in page.

17 23. CLEAR offers users the ability to conduct numerous types of searches for a targeted  
18 individual or entity, including a "person search" and a "risk inform" search.

19 **CLEAR's Person Search:**

20 24. CLEAR prompts users conducting a "person search" to input information such as  
21 an individual's name, address, contact information, social security number, date of birth, age  
22 range, or driver's license number in order to locate a targeted individual.

23 25. The directions for filling out the "age range" field direct the user to enter "1 to 3  
24 digits," indicating that CLEAR permits searches for minors as well as adults.

25 \_\_\_\_\_  
26 <sup>8</sup> Thomson Reuters CLEAR Brochure, *available at*:  
27 [https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-](https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf)  
28 [brochure.pdf](https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf).

<sup>9</sup> Thomson Reuters, *CLEAR Plans and Pricing*, [https://legal.thomsonreuters.com/en/products/clear-](https://legal.thomsonreuters.com/en/products/clear-investigation-software/plans-pricing#corporate)  
[investigation-software/plans- pricing#corporate](https://legal.thomsonreuters.com/en/products/clear-investigation-software/plans-pricing#corporate).

1           26. The “person search” results bring the user to a landing page with personal  
2 identifying information. A column on the side of the screen includes the target individual’s full  
3 name, age, current address, and partial social security numbers; “vital statistics,” such as date  
4 of birth, gender, and former names; and former addresses and phone numbers.

5           27. The “person search” results page also features a dashboard of additional tools  
6 allowing a user to dive deeper into the targeted individual’s profile. The front page of the  
7 dashboard displays “possible quick analysis flags,” which indicate whether, according to  
8 CLEAR’s database, the individual’s profile includes various putative risk factors, such as  
9 bankruptcies, arrests, a criminal record, or “associate[s] or relative[s]” with arrests or criminal  
10 records.

11           28. CLEAR’s “web analytics” tool, available via the dashboard, permits the user to  
12 browse through images and profiles of the targeted person, as well as individuals with similar  
13 names. It also provides search hits for the targeted individual from websites. These results can  
14 be filtered by various metrics, including city, country, “FamilyRelation,” “PersonAttributes,”  
15 and “PersonRelationship.”

16           29. The “person search” dashboard also offers a number of other tools, such as a  
17 “graphical display” tool that provides visual depictions of the targeted individual’s legal  
18 history, as well as the individual’s relationship to registered agents, relatives, and other people  
19 with whom the individual shares phone numbers; an “associate analytics” tool exploring the  
20 personal information of a targeted individual’s purported family members and other  
21 “associates”; and a “map analytics” tool allowing a user to view all of the addresses associated  
22 with the targeted individual on a detailed map, which includes satellite imagery.

23           30. Users may also create a report from the results of the “person search,” including  
24 detailed information not only about the targeted individual, but also that person’s relatives,  
25 “associates,” neighbors, addresses, properties, vehicles, and businesses in the report.

26           **CLEAR’s Risk Inform Search:**

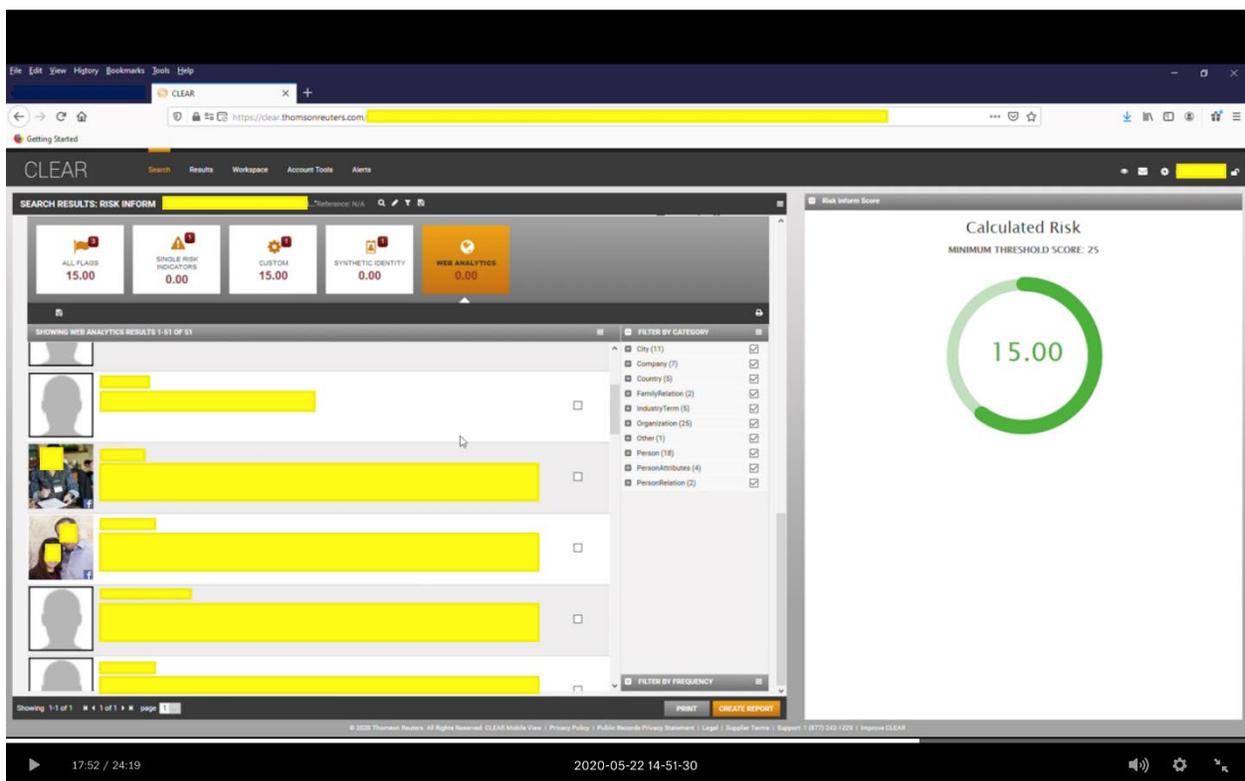
27           31. CLEAR’s “risk inform” search creates a detailed report of the putative risks  
28

1 associated with a targeted individual, summarizing a person’s purported “risk” using a  
2 numerical score.<sup>10</sup> A “risky” person has a high score, while a “safe” person has a low score.

3 32. The age range field for the “risk inform” search directs users to enter “1 to 3 digits,”  
4 again indicating that this tool may be used to profile minors as well as adults.

5 33. The “risk inform” results include the same “vital statistics,” address, contact  
6 information, web analytics information, and photographs that CLEAR provides in a “person  
7 search.”

8 34. In addition, the “risk inform” results include an automatically generated “risk  
9 inform score.”



10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24 35. The potential “flags” identified as components of this score demonstrate the breadth  
25 and sensitivity of the information included in the CLEAR database. For instance, under a list of  
26 “custom” flags, which appear to be associated with a wide range of state criminal offenses:

27  
28 <sup>10</sup> Thomson Reuters, *CLEAR Risk Inform*, <https://legal.thomsonreuters.com/en/products/clear-investigation-software/clear-risk-inform>.

- 1 a. CLEAR includes indicators for several types of conduct related to “Abortion,”  
2 including “Abortional Act on Self”;
- 3 b. Under the header “Breach of the Peace,” CLEAR includes indicators for speech and  
4 protest-related activity, including “Anarchism,” “Desecrating a Flag,” and  
5 “Engaging in a Riot,” and in subsequent sections, it also identifies “Indecent,  
6 Obscene, or Vulgar Language” and “Refusing to Aid a Police Officer”;
- 7 c. CLEAR includes indicators for “Homosexual Act with a Man” and “Homosexual  
8 Act with a Woman”;
- 9 d. Under the header “Weapons Offenses,” CLEAR includes indicators for “Licensing  
10 - Registered Weapon” and “Possession of a Weapon”; and
- 11 e. CLEAR also includes flags for intrusive conduct under the header “Invasion of  
12 Privacy.”<sup>11</sup>

13 36. Several of CLEAR’s “risk inform” flags are automatically triggered if the targeted  
14 individual changes their name, as illustrated by the dossiers on both of the named plaintiffs  
15 described below. Members of groups that are more likely to change their names—such as  
16 women who marry, victims of domestic violence, trans people, and Muslim converts—are  
17 thereby more likely to be tagged as “risky” by CLEAR’s “risk inform” product.

18 37. Clicking on any of the “risk inform” flags enables the user to see additional  
19 information about the alleged offense or trigger.

20 38. As with the “person search,” CLEAR permits users to generate a report of the “risk  
21 inform” results that may include information about the targeted individual as well as their  
22 relatives, associates, and neighbors.

23  
24  
25 <sup>11</sup> Although it has been held unconstitutional to use several of the items identified under “Criminal Records” as  
26 the basis for a criminal charge, it is unclear whether CLEAR determines whether these “flags” are triggered strictly  
27 using criminal records and whether it takes account of whether charges have subsequently been sealed or  
28 expunged. Moreover, it is unlikely that CLEAR’s algorithm discounts criminal charges in its database that predate  
changes in the criminal code (e.g., a charge for private homosexual conduct that preceded the Supreme Court’s  
ruling in *Lawrence v. Texas*, 539 U.S. 558 (2003)).



1 name change, including “Duplicate Personally Identifiable Information,” “First Appearance in  
2 Public Records content after 30,” “SSN Matched to Multiple Individuals,” and “Thinness of  
3 File.” As a result, Ms. Brooks is saddled with a high “risk inform” score, indicated in bold red.  
4 CLEAR’s “individual report” of information associated with Ms. Brooks’ prior name is also  
5 extensive.

6 45. CLEAR also provides photographs of Ms. Brooks.

7 46. At the bottom of a Thomson Reuters’ webpage about CLEAR—only visible after  
8 scrolling past two or more pages of text—there is a link in very small font that says: “For CA:  
9 Do not sell my information.”<sup>12</sup>

10 47. Clicking on the link sends visitors to a page that purports to allow California  
11 residents to opt out of the sale of their “personal information” for a period of “at least twelve  
12 (12) months.”

13 48. Beyond its presence in tiny font at the very bottom of its webpages, Thomson  
14 Reuters provides no notice to consumers that this link exists. Nor does the company enable  
15 California consumers who happen to find out about the link to easily make use of it.<sup>13</sup>

16 49. Ms. Brooks clicked the “For CA: Do not sell my information” link, seeking to opt out  
17 of the sale of her personal information via CLEAR. However, when she attempted to do so,  
18 Thomson Reuters required that she provide a photograph of her government-issued  
19 identification card as well as a separate picture of her face. Given that Thomson Reuters is  
20 already selling her personal information without her consent, Ms. Brooks was not comfortable  
21 providing further personal information to the company, and thus she could not complete the  
22 company’s process.

23 **Rasheed Shabazz:**

24 50. Named plaintiff Rasheed Shabazz is a Black Muslim journalist and activist. He is  
25

26 <sup>12</sup> <https://legal.thomsonreuters.com/en/products/clear-investigation-software>.

27 <sup>13</sup> Several Thomson Reuters webpages also include a second link at the bottom of the page that say: “Do not sell  
28 my personal information.” Clicking on one of these links brings up a pop-up window that states that the  
personal information to which it refers is information collected by cookies stored on the visitor’s browser “to  
collect information.”

1 concerned about being targeted by people who disagree with his writing, his teaching, and his  
2 activism, as well as by people who simply dislike his identity. He does not want his personal  
3 information to be publicly available.

4 51. Mr. Shabazz did not give Thomson Reuters consent to include his identity and  
5 identifying information in the CLEAR database. Thomson Reuters neither asked Mr. Shabazz  
6 for permission to sell his identifying information, nor paid Mr. Shabazz for the right to sell it.

7 52. Mr. Shabazz does not want Thomson Reuters to profit from his identity. He also  
8 does not want Thomson Reuters to present the story of his life to others without his input.

9 53. But CLEAR's "individual report" on Mr. Shabazz includes detailed information  
10 such as his current and prior addresses, employer information, phone numbers, a partially  
11 redacted social security number, his "associates," his neighbors—and their addresses and  
12 phone numbers.

13 54. Because, in Mr. Shabazz's view, the last name he was given at birth was associated  
14 with the slave owners who held his ancestors in bondage, Mr. Shabazz legally changed his  
15 name to one he felt was a better representation of himself and his family. CLEAR includes  
16 detailed information associated with Mr. Shabazz's prior name, including the same partially  
17 redacted social security number, his race, and physical addresses, email addresses, and phone  
18 numbers. Some of this information is inaccurate: CLEAR's profile on Mr. Shabazz's prior name  
19 indicates that Mr. Shabazz was divorced, when he has never legally been married, and that he  
20 has been sued for failing to pay child support, when he has no children.

21 55. Like Ms. Brooks, CLEAR's "risk inform" report penalizes Mr. Shabazz for changing  
22 his name: His "risk inform score" is based on flags indicating "First Appearance in Public  
23 Records after 30," "No relatives," and "SSN Matched to Multiple Individuals."

24 56. CLEAR provides photographs of Mr. Shabazz, including a profile picture CLEAR  
25 has chosen for the account they sell.

26 57. Mr. Shabazz also attempted to opt out of the sale of his personal information by  
27 clicking the "For CA" link provided at the bottom of Thomson Reuter's webpages. However,  
28

1 when he attempted to do so, Thomson Reuters required that he provide a photograph of his  
2 government-issued identification card as well as a separate picture of his face. Given that  
3 Thomson Reuters was selling his personal information without his consent, Mr. Shabazz was  
4 not comfortable providing further personal information to the company, and thus he could not  
5 complete the company's process.

6 *Thomson Reuters makes substantial profits from its sale of personal data and identifying*  
7 *information through CLEAR*

8 58. Thomson Reuters markets the CLEAR platform to individuals, private corporations,  
9 law enforcement, and other government agencies.

10 59. Thomson Reuters stores and collects CLEAR data in one or more of its Strategic Data  
11 Centers. To access this data, an individual can pay for a monthly subscription for one or more  
12 of Thomson Reuters' CLEAR data "plans." A customer can also choose to pay per individual  
13 search, demonstrating the value that each individual profile in CLEAR's database holds for  
14 Thomson Reuters. CLEAR offers tailored subscription plans for law enforcement, government  
15 agencies, and private corporations, respectively. Thomson Reuters charges individual users a  
16 monthly rate for access to its many CLEAR programs.

17 60. Thomson Reuters makes significant profits from the collection, aggregation, and  
18 sale of individuals' names, photographs, likenesses, identifying information, and personal data  
19 through its CLEAR products.

20 61. Thomson Reuters charges users for each component of CLEAR's search  
21 functionalities. It offers both flat rate and "pay-as-you-go" pricing models, with a minimum  
22 contract term of twelve months.<sup>14</sup>

23 62. In Thomson Reuter's "pay-as-you-go" pricing model, users pay per each component  
24 of a search and per report. For instance, in one pricing schedule, Thomson Reuters indicated  
25 that users would pay \$5.00 for a basic "Person Search," with additional charges added for  
26 additional information. According to this schedule, users also incur additional charges for a

27 \_\_\_\_\_  
28 <sup>14</sup> Thomson Reuters, *CLEAR Plans and Pricing*, <https://legal.thomsonreuters.com/en/products/clear-investigation-software/plans-pricing#corporate>.

1 “Photo Line-Up Search” and a “Web Analytics Search.” Thomson Reuters also charges  
2 separately to use CLEAR’s “Risk Inform” product, up to \$6.75 for a “premium” search. And  
3 users must also pay additional fees to generate reports from their searches: An “individual  
4 report” costs \$15.00, with additional charges added to include “associates” or “Risk Inform”  
5 data in the report.<sup>15</sup>

6 63. Government records offer another glimpse into the revenues that Thomson Reuters  
7 derives from its sale of CLEAR products. U.S. Immigration and Customs Enforcement (“ICE”)  
8 has signed over \$54 million in contracts with Thomson Reuters to access CLEAR for purposes  
9 of surveilling and tracking immigrants.

10 *Thomson Reuters is aware of the privacy concerns posed by its appropriation and sale of*  
11 *individuals’ personal data without their consent*

12 64. Thomson Reuters knows that its aggregation and sale of personal data without  
13 consent implicate significant privacy concerns.

14 65. In an article posted on its website for “insights” on “legal” issues, Thomson Reuters  
15 acknowledges the negative privacy consequences that flow from the non-consensual sale of a  
16 person’s personal data. As it explains, “[s]econdary uses of personal data” – that is, uses of a  
17 person’s data for purposes the person didn’t intend or consent to – “pose the most risk and  
18 unintended harm to people.” Individuals are blindsided by these secondary uses because they  
19 rightfully assume that even if their personal information has been uploaded somewhere, that  
20 “doesn’t mean permission has been given to share that information everywhere.”<sup>16</sup>

21 66. By the company’s own admission, “the amount of digital data being collected and  
22 stored” by corporations that profit off of personal data has reached “unprecedented rates.”  
23 Data analytics, a service which the company provides to its CLEAR customers, “has enormous  
24 power to reveal seemingly hidden patterns.” According to Thomson Reuters, data analytics  
25 processes can be so invasive that their insights “can even predict behavior,” thereby

26 \_\_\_\_\_  
27 <sup>15</sup> Thomson Reuters, *CLEAR Services Schedule A Commercial Subscriber’s Accessing Enhanced CLEAR Services*,  
<https://static.legalsolutions.thomsonreuters.com/static/agreement/schedule-a-clear.pdf>.

28 <sup>16</sup> Thomson Reuters, *Big Data ethics: redefining values in the digital world*,  
<https://legal.thomsonreuters.com/en/insights/articles/big-data-ethics-redefining-values-in-the-digital-world>.

1 “threaten[ing] individual identity.”<sup>17</sup>

2 67. Because CLEAR’s database is privately owned, it is not subject to the privacy  
3 protections that apply to government collection and storage of personal data. Commentators  
4 have observed that government agencies like ICE and local law enforcement may be able to  
5 avoid constitutional and statutory limitations by purchasing personal data from data brokers  
6 and other private companies like Thomson Reuters.<sup>18</sup>

7 68. Despite Thomson Reuters’ awareness that consent should be acquired before  
8 sharing personal information, the company never asks the individuals whose information is  
9 contained in the CLEAR database for their consent.

10 69. In fact, most individuals have no way of knowing that Thomson Reuters has bought,  
11 collected, aggregated, or sold their personal data.

#### 12 CLASS ACTION ALLEGATIONS

13 70. Under Code of Civil Procedure section 382 and Rule of Court 3.760 *et seq.*, the  
14 plaintiffs bring claims one, two, and three of this action on behalf of themselves and the  
15 following proposed class:

16 All persons residing in the state of California whose name, photographs, personal  
17 identifying information, or other personal data is or was included in the CLEAR  
18 database during the limitations period.

19 71. The proposed class definition excludes any officers and directors of Thomson  
20 Reuters; Class Counsel; and the judicial officer(s) presiding over this action and the members  
21 of his/her immediate family and judicial staff.

22 72. The number of class members is unknown to the plaintiffs, but it likely includes  
23 nearly all Californians. In light of Thomson Reuters’ claims that the CLEAR database contains  
24 “billions of data points,” including more than 140 million booking records and over 38 million  
25 images of individuals, the class is so numerous that joinder of all members is impractical.

---

26  
27 <sup>17</sup> *Id.*

28 <sup>18</sup> Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, Wired (Feb. 11, 2020),  
<https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/>.

1 73. There are questions of law and fact common to the class, which predominate over  
2 any questions affecting only individual class members. These questions include, but are not  
3 limited to, the following:

- 4 a. Whether Thomson Reuters' collection and sale of personal data through the CLEAR  
5 platform violates California's common law right of publicity.
- 6 b. Whether Thomson Reuters' collection and sale of personal data through the CLEAR  
7 platform violates California's Unfair Competition Law, Cal. Bus. & Prof. § 17200, *et*  
8 *seq.*
- 9 c. Whether Thomson Reuters has a process for obtaining consent before collecting,  
10 aggregating, and selling individuals' personal data in the CLEAR database.
- 11 d. Whether Thomson Reuters' sale of personal data through the CLEAR platform  
12 constitutes a misappropriation for commercial advantage under California law.
- 13 e. Whether class members' names, photographs, and other identifying information are  
14 directly connected to the commercial purpose of selling access to that information.
- 15 f. The extent to which Thomson Reuters has profited from the non-consensual sale of  
16 personal identifying information and data.

17 74. These and other legal and factual questions are common to all class members. There  
18 are no individual questions that will predominate over common questions.

19 75. The plaintiffs will fairly and adequately protect the interests of the class because  
20 their interests are aligned with, and not antagonistic to, those of the other members of the class.  
21 In addition, the plaintiffs have retained counsel experienced in handling class claims and claims  
22 involving unlawful business practices. Neither the plaintiffs nor their counsel have any  
23 interests which might cause them not to vigorously pursue this claim.

24 76. The plaintiffs' claims are typical of the claims of the members of the class. The  
25 plaintiffs and the class members sustained damages arising out of the defendant's common  
26 course of unlawful conduct. The damages and injuries of each class member were directly  
27 caused by the defendant's wrongful conduct.



1 85. At no time has Thomson Reuters sought consent from class members before  
2 appropriating and selling their personal data through its CLEAR products, nor does it have a  
3 process for doing so.

4 86. The class members received no compensation for Thomson Reuters' use of their  
5 identities.

6 87. Thomson Reuters' appropriation and sale of the plaintiffs' and class members'  
7 names, photographs, likenesses, and personal information without their consent injured the  
8 class members by violating their privacy. In particular, Thomson Reuters has prevented – and  
9 continues to prevent – the named plaintiffs and class members from retaining control over the  
10 dissemination of their personal information.

11 88. The named plaintiffs and the class members have also suffered economic injury  
12 because they were not compensated by Thomson Reuters for the use of their name,  
13 photographs, likeness, and other personal identifying information.

14 89. The named plaintiffs and class members are entitled to compensatory damages,  
15 restitution, declaratory relief, and injunctive relief.

## 16 SECOND CAUSE OF ACTION

### 17 Unfair Competition Law, Cal. Bus. & Prof. § 17200, Monetary Relief

18 90. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully  
19 stated herein.

20 91. California Business and Professions Code section 17200 *et seq.* ("UCL") prohibits  
21 "unlawful, unfair, or fraudulent business acts or practices."

22 92. By selling Californians' personal information and data without consent, as  
23 described above, Thomson Reuters has engaged in unlawful and unfair acts and practices  
24 prohibited by the UCL.

25 93. Thomson Reuters' conduct is unlawful under the UCL because it violates  
26 California's common-law right of publicity, as discussed in the first cause of action.

27 94. In addition, Thomson Reuter's conduct is unlawful under the UCL because it  
28

1 violates California Civil Code section 3344(a).

2 95. California Civil Code section 3344(a) provides that “[a]ny person who knowingly  
3 uses another’s name, voice, signature, photograph, or likeness, in any manner, on or in  
4 products, merchandise, or goods, . . . without such person’s prior consent . . . shall be liable for  
5 any damages sustained by the person or persons injured as a result thereof.”

6 96. Thomson Reuters knowingly used and continues to use the names, photographs,  
7 and other identifying information of the class members in its CLEAR database, and for the  
8 purpose of selling access to products linked to the CLEAR database. Thomson Reuters’ use of  
9 this information is not an accident; it is central to these products.

10 97. Thomson Reuters’ appropriation of the class members’ names, photographs, and  
11 other identifying information was to the company’s economic and commercial advantage. The  
12 company has generated millions of dollars of revenue from CLEAR.

13 98. At no time has Thomson Reuters affirmatively sought consent from class members  
14 before appropriating and selling their personal data, nor does it have a process for doing so.

15 99. The class members received no compensation for Thomson Reuters’ use of their  
16 names, images, likenesses, and other personal identifying information.

17 100. Thomson Reuters’ use of class members’ names, photographs, and other identifying  
18 information is directly connected to its products’ commercial purposes: Products linked to the  
19 CLEAR database would be without value if the CLEAR database did not include class  
20 members’ names, photographs, and identifying information. Class members’ names,  
21 photographs, and identifying information are not ancillary to these products—they are the  
22 product.

23 101. Indeed, Thomson Reuters’ entire marketing strategy relies on emphasizing the vast  
24 quantity of photographs, names, and other identifying information that is readily available to  
25 potential subscribers of CLEAR. Thomson Reuters’ appropriation and sale of the named  
26 plaintiffs’ and class members’ names, photographs, likenesses, and personal information  
27 without seeking permission or consent injured the class members by violating their right to  
28

1 exercise control over the commercial use of their identities.

2 102. Thomson Reuters' conduct also constitutes unfair business practices under the UCL  
3 because these practices offend established public policy and cause harm to the named plaintiffs  
4 and class members, which cannot be reasonably avoided, and that outweighs any benefit to  
5 consumers or competition. The conduct also is immoral, unethical, oppressive, unscrupulous,  
6 and substantially injurious to consumers.

7 103. The named plaintiffs and class members have suffered economic injury as a result  
8 of Thomson Reuters' unlawful and unfair business practices.

9 104. As a result of its unlawful and unfair business practices, Thomson Reuters has  
10 reaped and continues to reap unfair and illegal profits at the expense of the plaintiffs and class  
11 members. Thus, Thomson Reuters should be required to disgorge its illegal profits, and to pay  
12 the plaintiffs and class members restitution in an amount according to proof at the time of trial.

### 13 **THIRD CAUSE OF ACTION**

#### 14 **Unjust Enrichment**

15 105. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully  
16 stated herein.

17 106. Thomson Reuters has wrongfully and unlawfully sold the named plaintiffs' and the  
18 class members' names, photographs, personal identifying information, and other personal data  
19 without their consent for substantial profits.

20 107. The named plaintiffs' and the class members' personal information and data have  
21 conferred an economic benefit on Thomson Reuters.

22 108. Thomson Reuters has been unjustly enriched at the expense of the named plaintiffs  
23 and class members, and the company has unjustly retained the benefits of its unlawful and  
24 wrongful conduct.

25 109. It would be inequitable and unjust for Thomson Reuters to be permitted to retain  
26 any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

27 110. The named plaintiffs and class members accordingly are entitled to equitable relief  
28

1 including restitution and disgorgement of all revenues, earnings, and profits that Thomson  
2 Reuters obtained as a result of its unlawful and wrongful conduct.

3 **FOURTH CAUSE OF ACTION**

4 **Unfair Competition Law, Cal. Bus. & Prof. § 17200, Public Injunctive Relief**

5 111. Plaintiffs reallege claims in the second cause of action for purposes of this action.

6 112. California Business and Professions Code section 17200 *et seq.* (“UCL”) prohibits  
7 “unlawful, unfair, or fraudulent business acts or practices.”

8 113. By selling Californians’ personal information and data without consent, as  
9 described above, Thomson Reuters has engaged in unlawful and unfair acts and practices  
10 prohibited by the UCL.

11 114. Thomson Reuters’ conduct is unlawful under the UCL because it violates California  
12 Civil Code section 3344(a) and California’s common-law right of publicity.

13 115. Thomson Reuters’ conduct also constitutes unfair business practices under the UCL  
14 because these practices offend established public policy and cause harm to the named plaintiffs  
15 and class members, which cannot be reasonably avoided, and that outweighs any benefit to  
16 consumers or competition. The conduct also is immoral, unethical, oppressive, unscrupulous,  
17 and substantially injurious to consumers.

18 116. California’s Unfair Competition Law allows anyone to bring an action for public  
19 injunctive relief if they have “lost money or property as a result of the unfair competition.” Cal.  
20 Bus. & Prof. § 17204.

21 117. Plaintiffs Brooks and Shabazz both lost money as a result of Thomson Reuters’  
22 unfair and unlawful practices in violation of the Unfair Competition Law. But for its violation  
23 of law, Thomson Reuters would have either paid Brooks and Shabazz for consent to sell their  
24 information or ceased the sale of their information.

25 118. Plaintiffs bring this fourth cause of action in a representative capacity, not on a class  
26 basis, seeking public injunctive relief to enjoin Thomson Reuter’s continued violation of  
27 California’s Unfair Competition Law.

1 **PRAYER FOR RELIEF**

2 For all of these reasons, the plaintiffs request that this Court:

- 3 a. Certify this action as a class action for purposes of Claims One through Three;
- 4 b. Appoint plaintiffs Cat Brooks and Rasheed Shabazz as class representatives and
- 5 appoint their attorneys as class counsel;
- 6 c. Award compensatory damages, declaratory relief, and injunctive relief;
- 7 d. Award restitution and disgorgement of the defendant’s profits from its unlawful
- 8 and unfair business practices and conduct;
- 9 e. Issue an order for public injunctive relief under the UCL, enjoining Thomson
- 10 Reuters from selling class members’ personal data without their consent, except for
- 11 legally permissible uses;
- 12 f. Award costs and reasonable attorneys’ fees; and
- 13 g. Grant such further relief that the Court deems necessary and proper.

14 **JURY DEMAND**

15 119. Plaintiffs demand a trial by jury for all issues so triable under the law.

16  
17  
18 DATED: December 3, 2020

Respectfully submitted,

19  
20 

21 Eric H. Gibbs (State Bar No. 178658)  
 22 Andre M. Mura (State Bar No. 298541)  
 23 Amanda M. Karl (State Bar No. 301088)  
 24 Jeffrey B. Kosbie (State Bar No. 305424)  
 25 Gibbs Law Group LLP  
 26 505 14th Street Suite 1110  
 27 Oakland CA 94612  
 28 (510) 350-9700  
 ehg@classlawgroup.com  
 amm@classlawgroup.com  
 amk@classlawgroup.com  
 jbk@classlawgroup.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Jennifer D. Bennett (State Bar No. 296726)  
Neil K. Sawhney (State Bar No. 300130)  
Gupta Wessler PLLC  
100 Pine Street, Suite 1250  
San Francisco, CA 94111  
(415) 573-0336  
*jennifer@guptawessler.com*  
*neil@guptawessler.com*

Benjamin Elga (*pro hac vice* forthcoming)  
Alice Buttrick (*pro hac vice* forthcoming)  
Justice Catalyst Law, Inc.  
81 Prospect St., 7th Floor  
Brooklyn, NY 11201  
(518) 732-6703  
*belga@justicecatalyst.org*  
*abuttrick@justicecatalyst.org*

Albert Fox Cahn (*pro hac vice* forthcoming)  
Surveillance Technology  
Oversight Project  
40 Rector Street, 9th Floor  
New York, NY 10006  
*albert@stopspying.org*

*Attorneys for Plaintiffs and the Proposed Class*