1   JONATHAN H. BLAVIN (State Bar No. 230269)
    jonathan.blavin@mto.com
2   NICHOLAS D. FRAM (State Bar No. 288293)
    nicholas.fram@mto.com
3   MUNGER, TOLLES & OLSON LLP
    560 Mission Street
4   Twenty-Seventh Floor
    San Francisco, California 94105-2907
5   Telephone: (415) 512-4000
    Facsimile: (415) 512-4077
6
    Attorneys for LinkedIn Corporation
7

8   UNITED STATES DISTRICT COURT

9   NORTHERN DISTRICT OF CALIFORNIA

10

11   LinkedIn Corporation,   Case No. 5:16-cv-4463

12   Plaintiff,   **Complaint For:**
                                             (1) VIOLATION OF THE COMPUTER
13   vs.   **FRAUD AND ABUSE ACT, 18 U.S.C.**
                                             §§ 1030 ET SEQ.;
14   Does, 1 through 100 inclusive,   **(2) VIOLATION OF CALIFORNIA**
                                             PENAL CODE §§ 502 ET SEQ.;
15   Defendants.   **(3) VIOLATION OF THE DIGITAL**
                                             MILLENNIUM COPYRIGHT ACT, 17
16   **U.S.C. §§ 1201 ET SEQ.;**
                                             (4) BREACH OF CONTRACT;
17   **(5) TRESPASS; AND**
                                             (6) MISAPPROPRIATION
18
                                             DEMAND FOR JURY TRIAL
19

20

21

22

23

24

25

26

27

28

1   Plaintiff LinkedIn Corporation ("LinkedIn" or "Plaintiff"), by and through its attorneys,

2   brings this Complaint against Defendants Does 1-100 (collectively, the "Doe Defendants") for

3   injunctive relief and damages. LinkedIn alleges as follows:

4   1.   LinkedIn is the world's largest professional network, with more than 400 million

5   members in over 200 countries and territories around the globe. LinkedIn's mission is to connect

6   the world's professionals to make them more productive and successful. Through its proprietary

7   platform, LinkedIn allows its members to create, manage and share their professional histories and

8   interests online.

9   2.   At the heart of LinkedIn's platform are its members, whose LinkedIn profiles serve

10   as their professional online identities. In order to protect the data that LinkedIn's members entrust

11   to LinkedIn, LinkedIn employs numerous technical measures designed to detect, limit, and block

12   "scraping" – the extraction and copying of data – on its website. LinkedIn's User Agreement also

13   prohibits "[s]crap[ing] or copy[ing] profiles and information of others" through "crawlers, browser

14   plugins and add-ons, and any other technology" used to access the LinkedIn website.

15   3.   During periods of time since December 2015, and to this day, unknown persons

16   and/or entities employing various automated software programs (often referred to as "bots") have

17   extracted and copied data from many LinkedIn pages. To access this information on LinkedIn's

18   site, the Doe Defendants circumvented several technical barriers employed by LinkedIn that

19   prevent mass automated scraping, and have knowingly and intentionally violated various access

20   and use restrictions in LinkedIn's User Agreement, which they agreed to abide by in registering

21   LinkedIn member accounts. In so doing, they have violated an array of federal and state laws,

22   including the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, et seq. (the "CFAA"),

23   California Penal Code §§ 502 et seq., and the Digital Millennium Copyright Act, 17 U.S.C. §§

24   1201 et seq. (the "DMCA"), and have engaged in unlawful acts of breach of contract,

25   misappropriation, and trespass.

26   4.   The Doe Defendants' unlawful conduct has harmed and threatens the LinkedIn

27   platform in several ways. First, their actions have violated the trust that LinkedIn members place

28   in the company to protect their information. Their unauthorized scraping also increased the strain

1   on LinkedIn's network servers and caused LinkedIn to expend time and resources investigating

2   and responding to their misconduct. Further, in aid of their illegal activities, the Doe Defendants

3   created thousands of fake LinkedIn profiles that polluted the LinkedIn user environment.

4   5.   LinkedIn has responded swiftly to the Doe Defendants' activities, including by

5   implementing additional technical barriers to the LinkedIn website to protect against mass

6   scraping and by promptly disabling fake member profiles. In addition to these measures, and to

7   ensure that future incidents do not occur, LinkedIn brings this action to identify the Doe

8   Defendants and to obtain permanent injunctive relief halting their unlawful conduct. The Doe

9   Defendants' activities, if not enjoined, threaten ongoing and irreparable harm to LinkedIn,

10 including to its reputation and substantial consumer goodwill. LinkedIn further is entitled to its

11 actual damages, statutory damages, and/or exemplary damages as a result of the Doe Defendants'

12 misconduct.

13   **JURISDICTION AND VENUE**

14   6.   This Court has federal question jurisdiction over this action under 28 U.S.C.

15 §§ 1331 and 1338 because this action alleges violations of federal statutes, including the CFAA,

16 18 U.S.C. §§ 1030, et seq., and the DMCA, 17 U.S.C. §§ 1201, et seq. The Court has

17 supplemental jurisdiction over the state law causes of action pleaded herein pursuant to 28 U.S.C.

18 § 1367.

19   7.   Venue is proper in this District under 28 U.S.C. § 1391, because a substantial part

20 of the events or omissions giving rise to the claims occurred in this District.

21   8.   During all relevant times, the Doe Defendants have repeatedly, knowingly, and

22 intentionally targeted and accessed LinkedIn's servers located in this judicial district without

23 LinkedIn's authorization. While accessing LinkedIn's servers, the Doe Defendants have had

24 systematic and continuous contacts with this judicial district, and targeted their wrongful acts at

25 LinkedIn, which is headquartered in this judicial district.

26   9.   The Doe Defendants also have agreed to LinkedIn's User Agreement, which

27 contains a forum selection clause selecting this judicial district for resolution of all disputes

28 between the parties.

1

INTRADISTRICT ASSIGNMENT

2   10.   This is an intellectual property action to be assigned on a district-wide basis under

3   Civil Local Rule 3-2(c).

4

THE PARTIES

5   11.   LinkedIn is a Delaware corporation with its principal place of business in Mountain

6   View, California.

7   12.   The Doe Defendants are persons and/or entities responsible in whole or in part for

8   the wrongdoing alleged herein. At least for some of the unlawful acts alleged herein, the Doe

9   Defendants registered member accounts on LinkedIn, subject to the LinkedIn User Agreement.

10   LinkedIn is informed and believes that each of the Doe Defendants participated in, ratified,

11   endorsed, or was otherwise involved in the acts complained of and that they have liability for such

12   acts. LinkedIn intends to seek expedited discovery to learn the identity of the Doe Defendants and

13   will amend this Complaint if and when the identities of such persons or entities and/or the scope of

14   their actions becomes known.

15

FACTS

16

The LinkedIn Professional Network

17   13.   LinkedIn is the world's largest professional network, with over 400 million

18   members worldwide and over 128 million members in the United States. LinkedIn's mission is to

19   connect the world's professionals to make them more productive and successful.

20   14.   Through its proprietary platform, LinkedIn members are able to create, manage

21   and share their professional identities online, build and engage with their professional network,

22   access shared knowledge and insights, and find business opportunities, enabling them to be more

23   productive and successful. LinkedIn's broader vision is to create economic opportunity for every

24   member of the global workforce.

25   15.   At the heart of LinkedIn's platform are its members, who create individual profiles

26   that serve as their professional profiles online.   LinkedIn is available at no cost to anyone who

27   wants to join and who agrees to the terms of LinkedIn's User Agreement, Privacy Policy, and

28   Cookie Policy. LinkedIn counts executives from all 2015 Fortune 500 companies as members.

-3-
COMPLAINT

16.   LinkedIn members populate their profiles with a wide range of information concerning their professional lives, including summaries (narratives about themselves), job histories, skills, interests, educational background, professional awards, photographs, and other information.

17.   The LinkedIn website is an original copyrighted work. Among the significant original elements of the LinkedIn website are the distinctive page layout, design, graphical elements, and organization of member and company profile pages and the LinkedIn homepage and news feed.

18.   LinkedIn has invested and plans to continue to invest substantial time, labor, skill, and financial resources into the development and maintenance of the LinkedIn site.

**LinkedIn's Technical Safeguards and Security Measures
to Protect LinkedIn Against Unauthorized Access**

19.   LinkedIn works hard to protect the integrity and security of its network and systems. Among other things, it employs an array of technological safeguards and barriers designed to prevent data scrapers, bots and other automated systems from accessing and copying its members' data on a large scale.

20.   One such safeguard is LinkedIn's FUSE system. FUSE scans and imposes a limit on the activity that an individual LinkedIn member may initiate on the site. This limit is intended to prevent would-be data scrapers utilizing automated technologies from quickly accessing a substantial volume of (public or private) member profiles.

21.   Another safeguard is LinkedIn's Quicksand system. Quicksand monitors the patterns of webpage requests by LinkedIn members in order to identify non-human activity indicative of scraping. Quicksand can quickly challenge or restrict the account to prevent scrapers from continuing to access the site.

22.   Another protection measure is LinkedIn's Sentinel system, which scans, throttles, and at times blocks suspicious activity associated with particular IP addresses.[1]

---

[1] An IP address in this context is a numerical label assigned to each access point to the Internet.

1   23.   LinkedIn also monitors and blocks groups of IP addresses using its Org Block

2 system. This system includes an evolving manual list of known bad IP addresses and a machine-

3 learned model that identifies groups of IP addresses serving large-scale scrapers. At the same

4 time, and consistent with industry practice, LinkedIn "whitelists" a number of popular and

5 reputable service providers, search engines, and other platforms so as to permit them to query and

6 index the LinkedIn website, without being subject to all of LinkedIn's security measures.

7   24.   LinkedIn also employs Member and Guest Request Scoring systems, which also

8 restrict automated, non-human forms of access that facilitate scraping. The Member Request

9 Scoring System monitors page requests made by LinkedIn members while logged into their

10 accounts. If high levels of activity are detected for certain types of accounts, the member is

11 logged out and may either be warned, restricted, or challenged with a CAPTCHA[2] in order to log

12 back into LinkedIn.

13   25.   Similarly, the LinkedIn Guest Request Scoring system monitors and limits page

14 requests made by users who are not logged into LinkedIn. If unusual patterns or high levels of

15 activity are detected, the user is redirected to LinkedIn's log-in page and is prevented from

16 viewing additional LinkedIn pages while not logged in.

17   26.   LinkedIn also has anticipated that data scrapers might attempt to create a multitude

18 of fake member accounts. Accordingly, as additional layers of protection, LinkedIn employs

19 several additional technical barriers, including its UCV system, to thwart this misconduct. The

20 UCV system uses a number of parameters to determine if a new account signup is suspicious. If a

21 suspicious signup is identified, the UCV system imposes barriers intended to separate legitimate

22 prospective members from automated data scraping programs and bots. The UCV system

23 introduces a CAPTCHA field that requires prospective members to re-type a word or text that

24 appears in obscured, colored type. These obscured words or text are legible to a real person – and

25 familiar to those purchasing concert tickets, for instance, as a common step in an online
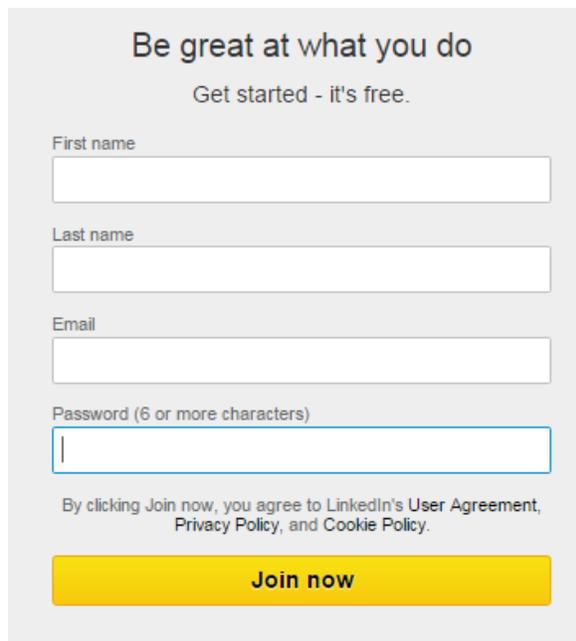
26

27 _____

[2] CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and
28 Humans Apart."

-5-

1   registration process – but difficult for an automated program or bot to recognize. By using

2   CAPTCHAs, the UCV system prevents data scrapers from automatically registering many new

3   and illegitimate member accounts.

4   **LinkedIn's Prohibitions on Data Scraping and Other Unauthorized Conduct**

5   27.   LinkedIn's User Agreement[3] also prohibits accessing and scraping LinkedIn's

6   website through automated software and other technologies, and the creation and use of fake

7   member accounts.

8   28.   As demonstrated by the screenshot below, a prospective member registers for an

9   account by providing a first name, last name, email address, and password, and through clicking

10 "Join Now," "agree[s] to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy," all of

11 which are hyperlinked on the page.

12

13   Be great at what you do

                                 Get started - it's free.

14   First name

15   _____

            Last name

16   _____

17   Email

            _____

18   Password (6 or more characters)

19 | _____

20   By clicking Join now, you agree to LinkedIn's User Agreement,
            Privacy Policy, and Cookie Policy.

21   **Join now**

22

23   29.   As described further below, the Doe Defendants registered thousands of fake

24 member accounts as part of their data scraping activities. For each of those accounts, the Doe

25 Defendants agreed to be bound by LinkedIn's User Agreement.

26   30.   LinkedIn's User Agreement explains that members, users, and visitors to the

27 _____
    [3] *See* https://www.linkedin.com/legal/user-agreement.

28

-6-

COMPLAINT

1   LinkedIn website must abide by certain restrictions in accessing and using the LinkedIn website.

2   31.   Section 8.2 of the current version of the User Agreement, effective October 23,

3   2014, prohibits those who are bound to the agreement from engaging in any of the following

4   activities:

5   •   "Us[ing] … automated software, devices, scripts robots, other means or processes to

6   access, 'scrape,' 'crawl' or 'spider' the Services or any related data or information";

7   •   "Us[ing] bots or other automated methods to access the Services";

8   •   "Scrap[ing] or copy[ing] profiles and information of others" through "crawlers, browser

9   plugins and add-ons, and any other technology";

10   •   "Rent[ing], leas[ing], loan[ing], trad[ing], sell[ing]/re-sell[ing] access to the Services or

11   related any information or data";

12   •   "Creat[ing] a false identity on LinkedIn";

13   •   "Creat[ing] a Member profile for anyone other than yourself (a real person)";

14   •   "Us[ing] or attempt[ing] to use another's account";

15   32.   In Section 2.1 of the User Agreement, members also agree that they "will only have

16   one LinkedIn account . . . which must be in your real name" and that they are "not already

17   restricted by LinkedIn from using" the LinkedIn website.

18   33.   As demonstrated below, the Doe Defendants have engaged in a systematic pattern

19   of conduct in violation and breach of each of these provisions of the User Agreement.

20   **The Doe Defendants' Unlawful Data Scraping Activities**

21   34.   During periods of time since December 2015, and to this day, the Doe Defendants

22   have created and/or utilized a highly coordinated and automated network of computers (a

23   "botnet") distributed across dozens of Internet Service Providers ("ISPs") and networks, and many

24   thousands of IP addresses. These ISPs and networks span the range of local, regional, and

25   national providers in this country and abroad.

26   35.   In engaging in this conduct, the Doe Defendants have accessed LinkedIn's website

27   and scraped data from many LinkedIn pages in circumvention of several of LinkedIn's

28   technological defenses and in violation of the access and use restrictions in LinkedIn's User

1   Agreement.

2   36.   First, through utilizing large sets of distributed networks and IP addresses that

3   change frequently, the Doe Defendants have circumvented the technical restrictions that LinkedIn

4   places on the amount of activity users may initiate, such as FUSE, Quicksand, and the Member

5   and Guest Request Scoring systems. This has allowed them to engage in highly automated

6   queries, scraping, and other conduct which from any particular account or IP address are less than

7   the total number of permitted activities over a period of time. Such activity circumvents

8   LinkedIn's automated restriction levels, yet allows the Doe Defendants to engage in equivalent

9   levels of banned automated conduct.

10   37.   Further, through utilizing a network of thousands of IP addresses and anonymizing

11 their true identity and IP address location, the Doe Defendants have circumvented LinkedIn's

12 technical protection measures that monitor and block suspicious activity associated with particular

13 IP addresses, including Sentinel and the Org Block system. This also has allowed the Doe

14 Defendants to mask their true identity.

15   38.   In addition to using a botnet, the Doe Defendants also have fraudulently directed

16 some of their scraping activity through a "whitelisted" entity, thereby circumventing LinkedIn's

17 security measures. The Doe Defendants were able to manipulate a whitelisted third-party cloud

18 service provider through which they directed a large number of requests to LinkedIn servers.

19 Doing so circumvented the technical barriers described above because LinkedIn servers were

20 programmed to permit higher volumes of server requests from this whitelisted partner.

21   39.   At the same time, the Doe Defendants circumvented the UCV system by using

22 automated technologies to register thousands of fake member accounts without triggering and

23 thereby evading the UCV system's imposition of CAPTCHAs.

24   40.   In creating and registering their accounts, the Doe Defendants agreed to abide by

25 the access and use restrictions in LinkedIn's User Agreement. The Doe Defendants' conduct, as

26 described above, violates several provisions of the User Agreement, including that LinkedIn

27 members and users would not use "automated software, devices, scripts robots, other means or

28 processes to access, 'scrape,' 'crawl' or 'spider' the Services or any related data or information."

-8-

1 Similarly, in creating the fake accounts, the Doe Defendants have violated the provisions in the

2 User Agreement providing that LinkedIn members and users will not create a "false identity on

3 LinkedIn" and will "only have one LinkedIn account . . . which must be in your real name." The

4 Doe Defendants knowingly violated these access and use restrictions in engaging in their unlawful

5 conduct.

6   41.   The Doe Defendants did not have permission or authorization from any LinkedIn

7 members, or from LinkedIn, at any point in time to access their member profiles and scrape their

8 data on LinkedIn through these automated technologies.

9   **LinkedIn's Response**

10   42.   LinkedIn has conducted and has continued to engage in an extensive investigation

11 of the Doe Defendants' continuing misconduct. In the course of its investigation, it has compiled

12 spreadsheets and other reports tracking the ISPs, networks, and IP addresses used by the Doe

13 Defendants, the dates and times of the Doe Defendants' activity on the LinkedIn website, and the

14 number of pages accessed by the Doe Defendants. LinkedIn also has identified fake member

15 profiles believed to have been created by the Doe Defendants. LinkedIn has disabled the fake

16 member profiles it has identified and implemented additional technical safeguards to protect

17 against unauthorized access to the LinkedIn site.

18   43.   Based on its investigation, LinkedIn also has collected information regarding the

19 whitelisted cloud computing platform that the Doe Defendants manipulated in order to circumvent

20 LinkedIn's technical barriers.

21   44.   LinkedIn expects to be able to identify the Doe Defendants by serving third-party

22 discovery on various ISPs and networks. These entities are in possession of information that will

23 help LinkedIn identify the Doe Defendants. LinkedIn intends to file a motion to expedite these

24 discovery requests.

25   **The Doe Defendants Have Caused and Threaten Ongoing and Irreparable**
                                      Injury to LinkedIn
26
          45.   By engaging in the activities described above, the Doe Defendants have caused,
27
   and if not halted will continue to cause, ongoing and irreparable harm to LinkedIn, in a variety of
28

1 ways, including ongoing and irreparable harm to its consumer goodwill.

2   46.   LinkedIn's members entrust LinkedIn their professional histories and interests on

3 LinkedIn's site. LinkedIn will suffer ongoing and irreparable harm to its consumer goodwill and

4 trust, which LinkedIn has worked hard for years to earn and maintain, if the Doe Defendants'

5 conduct continues.

6   47.   The Doe Defendants' misconduct also has imposed significant strains on

7 LinkedIn's servers, including through the use of automated technologies to view many LinkedIn

8 pages. The increased strain on LinkedIn's servers has impaired and reduced LinkedIn's ability to

9 serve legitimate LinkedIn users.

10   48.   The harm to LinkedIn's computer systems, including increased strain on its

11 network servers, and the significant human, financial, and technical resources, including hundreds

12 of hours of employee time, LinkedIn has expended investigating and responding to the Doe

13 Defendants' unlawful activities, has been at a cost to LinkedIn well in excess of $5,000.

14   49.   LinkedIn's members also expect the site to contain accurate and legitimate

15 professional profiles – not useless fictions crafted by data scrapers. The presence of fake member

16 profiles created by the Doe Defendants impairs legitimate members' ability to identify valid

17 professional contacts. This type of pollution to the LinkedIn network, if not halted, threatens

18 ongoing and irreparable harm to the integrity of the LinkedIn platform and LinkedIn's reputation.

19   **FIRST CLAIM FOR RELIEF**

20   **Computer Fraud and Abuse Act, 18 U.S.C. §§1030 et seq.**

21   50.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

22   51.   LinkedIn's computers and servers are involved in interstate and foreign commerce

23 and communication, and are protected computers under 18 U.S.C. §1030(e)(2).

24   52.   The Doe Defendants knowingly and intentionally accessed LinkedIn's computers

25 and servers without authorization or in excess of authorization. They have circumvented various

26 technological barriers LinkedIn has employed to protect its computers, servers, and member data

27 against unauthorized access – including FUSE, Sentinel, Org Block, the Member and Guest

28 Request Scoring systems, the UCV system, and/or additional safeguards – and have violated

1 access restrictions of LinkedIn's User Agreement.

2   53.   After accessing LinkedIn's computers and servers without authorization or in

3 excess of authorization, the Doe Defendants accessed, obtained and used valuable information

4 from LinkedIn's computers and servers in transactions involving interstate or foreign

5 communications in violation of 18 U.S.C. § 1030(a)(2). This information includes, among other

6 things, the contents of many LinkedIn profiles, and this use includes, among other things,

7 distributing that content to others.

8   54.   The Doe Defendants knowingly, willfully, and with an intent to defraud, accessed

9 LinkedIn's computers and servers without authorization or in excess of authorization, including

10 through masking the Doe Defendants' identity to LinkedIn's systems, and thereby furthered the

11 Doe Defendants' intended fraud and obtained valuable information from LinkedIn's computers

12 and servers that the Doe Defendants used to obtain something of value in violation of 18 U.S.C.

13 § 1030(a)(4).

14   55.   LinkedIn has suffered damage and loss by reason of these violations, including,

15 without limitation, harm to LinkedIn's computer systems, expenses associated with being forced

16 to investigate and respond to the unauthorized access and abuse of its computers and servers, and

17 other losses and damage in an amount to be proven at trial, in excess of $5,000 aggregated over a

18 one-year period.

19   56.   In addition, LinkedIn has suffered and will continue to suffer irreparable harm, and

20 its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe

21 Defendants. Accordingly, LinkedIn is entitled to injunctive relief.

22   **SECOND CLAIM FOR RELIEF**

23 **California Comprehensive Computer Access and Fraud Act, Cal. Penal Code §§ 502 et seq.**

24   57.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

25   58.   LinkedIn's computers and servers are computers, computer systems, and/or

26 computer networks within the meaning of Cal. Penal Code § 502(b).

27   59.   The Doe Defendants have circumvented various technological barriers LinkedIn

28 has employed to protect its computers, servers, and data against unauthorized access and use –

-11-

1   including FUSE, Sentinel, Org Block, the Member and Guest Request Scoring systems, the UCV

2   system, and/or additional safeguards – and have violated access and use restrictions of LinkedIn's

3   User Agreement.

4   60.   The Doe Defendants wrongfully obtained and used valuable information from

5   LinkedIn's website.

6   61.   The Doe Defendants knowingly and without permission accessed, took, copied and

7   made use of data and files from LinkedIn's computers, computer systems, and/or computer

8   networks, including to wrongfully control and/or obtain such data, in violation of Cal. Penal Code

9   §§ 502(c)(1) & (2).

10   62.   The Doe Defendants knowingly and without permission accessed or caused to be

11 accessed LinkedIn's computers, computer systems, and/or computer networks in violation of Cal.

12 Penal Code § 502(c)(7).

13   63.   The Doe Defendants knowingly and without permission disrupted or caused the

14 disruption of LinkedIn's computer services to authorized users of LinkedIn's computers,

15 computer systems, and/or computer networks in violation of Cal. Penal Code § 502(c)(5).

16   64.   As a direct and proximate result of the Doe Defendants' unlawful conduct, the Doe

17 Defendants have caused damage to LinkedIn in an amount to be proven at trial. LinkedIn is also

18 entitled to recover its reasonable attorney's fees pursuant to Cal. Penal Code § 502(e).

19   65.   LinkedIn believes that the Doe Defendants' acts were willful and malicious,

20 including that the Doe Defendants' acts described above were done with the deliberate intent to

21 harm LinkedIn. LinkedIn is therefore entitled to punitive damages.

22   66.   In addition, LinkedIn has suffered and will continue to suffer irreparable harm, and

23 its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe

24 Defendants. Accordingly, LinkedIn is entitled to injunctive relief.

THIRD CLAIM FOR RELIEF

The Digital Millennium Copyright Act, 17 U.S.C. §§ 1201 et seq.

27   67.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

28   68.   LinkedIn employs various layers of technological protections – including FUSE,

-12-

COMPLAINT

1 Sentinel, Org Block, the Member and Guest Request Scoring systems, the UCV system, and/or

2 additional safeguards – to protect LinkedIn's computers, servers, and data from unauthorized

3 access and copying, including through automated crawling and scraping technologies. These

4 technological protection measures effectively control access to the copyrighted materials on

5 LinkedIn's servers, including the LinkedIn website, member profile pages, company pages, and

6 the LinkedIn homepage and news feed, and protect LinkedIn's and its members' exclusive rights

7 in these copyrighted materials. These technological protection measures scan and monitor

8 accessing systems and require the application of information to confirm the absence of blocked IP

9 addresses, automated behavior patterns, server-origination data, and/or additional information,

10 with the authority of LinkedIn (on behalf of itself and its members), to gain access to the

11 copyrighted materials on LinkedIn's servers.

12   69.   Despite LinkedIn's best efforts to protect the LinkedIn site from the Doe

13 Defendants' unauthorized access, the Doe Defendants circumvented LinkedIn's technological

14 measures – including FUSE, Sentinel, Org Block, the Member and Guest Request Scoring

15 systems, the UCV system, and/or additional safeguards – and gained unauthorized access to

16 copyrighted materials, including without limitation the copyrighted LinkedIn website and member

17 profile pages, in violation of 17 U.S.C. § 1201(a)(1).

18   70.   As a result of the Doe Defendants' wrongful acts, LinkedIn has suffered, is

19 continuing to suffer, and will continue to suffer damages to be proven at trial. LinkedIn is further

20 entitled to all profits attributable to the Doe Defendants' wrongful acts to be proven at trial

21 pursuant to 17 U.S.C. § 1201(c).

22   71.   Alternatively, upon its election at any time before final judgment is entered,

23 LinkedIn is entitled to recover statutory damages from the Doe Defendants pursuant to 17 U.S.C.

24 § 1203, ranging from a minimum of $2,500 up to $25,000, for each act of circumvention

25 committed by the Doe Defendants. At a minimum, the Doe Defendants have engaged in

26 thousands of distinct acts of circumvention.

27   72.   The Doe Defendants' circumventions also have caused LinkedIn irreparable harm.

28 Unless restrained and enjoined, the Doe Defendants will continue to commit such acts.

COMPLAINT

1   LinkedIn's remedies at law are not adequate to compensate it for these inflicted and threatened

2   injuries, and thus LinkedIn is entitled to injunctive relief as provided by 17 U.S.C. § 1203.

3   <div align="center">**FOURTH CLAIM FOR RELIEF**</div>

4   <div align="center">**Breach of Contract**</div>

5   73.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

6   74.   Use of the LinkedIn website and use of LinkedIn services are governed by and

7   subject to the User Agreement.

8   75.   LinkedIn members are presented with the User Agreement and must affirmatively

9   accept and agree to the User Agreement to register for a LinkedIn account.

10   76.   At all relevant times, LinkedIn also prominently displayed a link to the User

11   Agreement on LinkedIn's homepage.

12   77.   The Doe Defendants accessed the LinkedIn website and affirmatively accepted and

13   agreed to the User Agreement to, among other things, create the fake member profiles that enabled

14   the Doe Defendants to access scrape data from LinkedIn's website.

15   78.   The User Agreement is enforceable and binding on the Doe Defendants.

16   79.   The Doe Defendants repeatedly accessed the LinkedIn website with knowledge of

17   the User Agreement and all of its prohibitions. Despite their knowledge of the User Agreement

18   and its prohibitions, the Doe Defendants accessed and continue to access the LinkedIn website to,

19   among other things, scrape, crawl, or use other automated technology or software to gain access to

20   the LinkedIn website without the consent of LinkedIn. Moreover, the Doe Defendants maintained

21   more than one account (indeed, thousands of accounts) at any given time, and did not provide their

22   real names or provide accurate information to LinkedIn.

23   80.   LinkedIn has been unable to contact the Doe Defendants to demand that they cease

24   and desist their data scraping and other LinkedIn-related activities because LinkedIn does not

25   know the identifies of the Doe Defendants.

26   81.   The Doe Defendants' actions, as described above, have willfully, repeatedly, and

27   systematically breached the User Agreement.

28   82.   LinkedIn has performed all conditions, covenants, and promises required of it in

<div align="center">-14-</div>
<div align="center">COMPLAINT</div>

1 accordance with the User Agreement.

2   83.   The Doe Defendants' conduct has damaged LinkedIn, and caused and continues to

3 cause irreparable and incalculable harm and injury to LinkedIn.

4   84.   LinkedIn is entitled to injunctive relief, compensatory damages, and/or other

5 equitable relief.

6 ## FIFTH CLAIM FOR RELIEF

7 **Trespass**

8   85.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

9   86.   The Doe Defendants intentionally, and without authorization, accessed and

10 interacted with LinkedIn, including without limitation, LinkedIn's website, computer systems and

11 servers.

12   87.   Through disregarding the prohibitions set forth in LinkedIn's User Agreement to

13 which they been on notice of and expressly consented to, and in circumvention of various

14 technical barriers, the Doe Defendants unlawfully gained access to and interfered and

15 intermeddled with LinkedIn, its website, computer systems, and its servers.

16   88.   The Doe Defendants' unauthorized interference with and access to LinkedIn, its

17 website, computer systems, and its servers, among other harms, has reduced LinkedIn's capacity

18 to service its users because it has occupied, used, and placed strain on LinkedIn's systems and

19 resources.

20   89.   The Doe Defendants' conduct constitutes trespass that has harmed and will

21 continue to harm LinkedIn. As a result, LinkedIn has been and will continue to be damaged.

22   90.   LinkedIn has suffered and will continue to suffer irreparable harm, and its remedy

23 at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants.

24 Accordingly, LinkedIn is entitled to injunctive relief.

25 ## SIXTH CLAIM FOR RELIEF

26 **Misappropriation**

27   91.   LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

28   92.   LinkedIn has invested substantial time, labor, skill, and financial resources into the

1 creation and maintenance of LinkedIn, its computer systems and servers, including system and

2 server capacity, as well as the content on the LinkedIn website, which is time sensitive. The Doe

3 Defendants have invested none of their own time and resources into developing and building the

4 LinkedIn website and platform.

5   93.   Disregarding the prohibitions set forth in LinkedIn's User Agreement to which

6 they have been on notice of and expressly consented to, and in circumvention of various technical

7 barriers, the Doe Defendants, without authorization, have wrongfully accessed LinkedIn's

8 website, computer systems and servers, and obtained data from the LinkedIn site.

9   94.   The Doe Defendants' appropriation and use of this data was at little or no cost to

10 the Doe Defendants, without them having to make the substantial investment in time, labor, skill,

11 and financial resources made by LinkedIn in developing the LinkedIn website and platform. In

12 other words, the Doe Defendants have reaped what they have not sown. The Doe Defendants' use

13 of LinkedIn's computer systems and servers, including member data from the LinkedIn site and

14 system and server capacity, constitutes free-riding on LinkedIn's substantial investment of time,

15 effort, and expense.

16   95.   As a result of this misappropriation, LinkedIn has been forced to expend additional

17 time and resources, including but not limited to, investigating and responding to the Doe

18 Defendants' activities, and the Doe Defendants have been able to exploit and benefit from

19 LinkedIn's substantial investment of time, effort, and expense.

20   96.   LinkedIn has been and will continue to be damaged as the result of the Doe

21 Defendants' acts of misappropriation.

22   97.   LinkedIn has suffered and will continue to suffer irreparable injury, and its remedy

23 at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants.

24   **PRAYER FOR RELIEF**

25   WHEREFORE, LinkedIn prays that judgment be entered in its favor and against the Doe

26 Defendants, as follows:

27   1.   A permanent injunction enjoining and restraining all the Doe Defendants, their

28 employees, representatives, agents, and all persons or entities acting in concert with them during

COMPLAINT

1   the pendency of this action and thereafter perpetually from

2   a.   accessing or using LinkedIn's website, servers, systems, and any data

3   displayed or stored therein, including through scraping and crawling technologies, for any

4   commercial purpose whatsoever; and

5   b.   extracting and copying data appearing on LinkedIn's website to their own

6   servers or systems or those controlled by them;

7   2.   An order requiring the Doe Defendants to destroy all documents, data, and other

8   items, electronic or otherwise, in their possession, custody, or control, that were wrongfully

9   extracted and copied from LinkedIn's website, along with any data that the Doe Defendants have

10   inferred as a result of data wrongfully extracted and copied from LinkedIn's website.

11   3.   An award to LinkedIn of damages, including, but not limited to, compensatory,

12   statutory, profits of the Doe Defendants, and/or punitive damages, as permitted by law;

13   4.   An award to LinkedIn of its costs of suit, including, but not limited to, reasonable

14   attorney's fees, as permitted by law; and

15   5.   Such other relief as the Court deems just and proper.

16   **DEMAND FOR JURY TRIAL**

17   LinkedIn hereby demands a jury trial of all issues in the above-captioned action that are

18   triable to a jury.

19   DATED: August 8, 2016   MUNGER, TOLLES & OLSON

20

21

22   By: */s/ Jonathan H. Blavin*
                                           JONATHAN H. BLAVIN
23

24   Attorneys for LinkedIn Corportation

25

26

27

28

-17-
COMPLAINT