VIA U.S. MAIL

Mayor Terry Tornek   City Manager Steven Mermell
100 N. Garfield Avenue, Room S228   100 N. Garfield Avenue
Pasadena, CA 91101   Pasadena, CA 91101

Chief Phillip L. Sanchez
Pasadena Police Department
207 N. Garfield Avenue
Pasadena, CA 91101

October 17, 2017

Re: **Public Records Act request related to City of Pasadena's use of Spokeo services**

To Mayor Tornek, City Manager Mermell, and Chief Sanchez,

On behalf of the ACLU of Southern California, I write to express the organization's serious concerns regarding the City of Pasadena's partnership with Spokeo, Inc. to provide its newly announced personal information and social media monitoring service for law enforcement (*Spokeo for Law Enforcement*) to the Pasadena Police Department.

Spokeo describes its monitoring software as "bring[ing] together public records and social media data" into a searchable interface for law enforcement agencies. This amounts to the maintenance of a massive, unregulated trove of personal information which raises significant civil liberties concerns, implicating the privacy and free speech rights of Pasadena residents. Surveillance technology proposals such as this one should not move forward without an open public debate about the civil liberties and civil rights costs. Members of the public should have the opportunity to scrutinize Spokeo's software, including its data sources and any decision-making algorithms it employs.

We urge the City not to obtain Spokeo for law enforcement purposes, at least until the concerns laid out below are addressed in robust and public debate. We further request the City provide all relevant documents concerning Spokeo pursuant to the California Public Records Act in order to make public Spokeo's capabilities and its service's risk to Pasadena residents' privacy.[1]

---

[1] This letter follows that written by ACLU Pasadena-Foothills Chapter dated August 14, 2017, which posed numerous questions about the City of Pasadena's interest in Spokeo's law enforcement service to the City's Public Safety Committee, as well as a meeting held by the ACLU with Chief Sanchez and Manager Mermell on September 26. As the City has not responded to that letter nor adequately addressed the questions raised in the September 26 meeting, we set forth our concerns more systematically here.

I.   Background

A.   Spokeo operates a "people search engine" that collects and organizes troves of public data about individuals and makes them available online.

Spokeo, Inc., a Pasadena-based technology company, operates a self-described online "people search engine" which allows end users to search for data on individuals scraped from "publicly available information from social networks, phone books, and real-estate and business websites."[2] Spokeo markets its "people search engine" to employers, realtors, debt collectors, non-profits, and individuals as a way of performing background checks, looking up personal details about others, monitoring updates about the lives of individuals, and unmasking anonymous communications.

Among the features of its search engine, Spokeo allows a user to "monitor" individuals and receive alerts to let the user know "when someone moves, when new contact info is added and when new social activity is found."[3] Spokeo previously described this feature as allowing customers access to alerts "whenever anyone has done anything new, anywhere online."[4] Indeed, its home page once advertised that its people engine helps individuals "uncover personal photos, videos, and secrets," including "juicy" and "mouth-watering news about friends and coworkers."[5]

A user might fairly presume that Spokeo, a company in the business of selling personal information organized "about people into simple and comprehensive online profiles," provides reliable data about individuals. [6] However, Spokeo's search results often display outdated, inaccurate, and stale information, and the company does not specifically ensure the accuracy of its data. As a result, the federal government sued Spokeo in 2012 alleging that the company violated the Fair Credit Reporting Act by failing to ensure the information contained in its vast database was accurate, not telling users about its obligations under the law, and failing to notify

---

[2] Mullin, Joe. "Appeals court: Lawsuit over wrong info on Spokeo should move ahead," Ars Technica (Aug. 16, 2017), https://arstechnica.com/tech-policy/2017/08/appeals-court-lawsuit-over-wrong-info-on-spokeo-should-move-ahead/.

[3] Spokeo, Inc. "Spokeo FAQs: 'What's included in the Spokeo app?'" (last visited Sep. 15, 2017), https://www.spokeo.com/faqs-consumer.

[4] Raphael, JR. "People Search Engines: They Know Your Dark Secrets … And Tell Anyone," PCWorld (Mar. 10, 2009), *available at* http://www.pcworld.com/article/161018/people_search_engines.html.

[5] *Id*.

[6] "Spokeo FAQs: 'What is Spokeo?'" Spokeo, Inc. (last visited Sep. 15, 2017), https://www.spokeo.com/faqs-consumer;

job seekers when employers decided not to hire them based on the data provided.[7] Spokeo settled the suit by agreeing to pay a fine of $800,000 and informing users that its data cannot be used to determine eligibility for credit, insurance, employment, or housing.[8]

In compliance with this settlement, Spokeo today disclaims any responsibility for the accuracy of the data it aggregates. It warns users of the following at the foot of every page of its website:

> Spokeo is not a consumer reporting agency as defined by the Fair Credit Reporting Act (FCRA). This site should not be used to make decisions about employment, tenant screening, or any purpose covered by the FCRA.

In addition, the response to the question "Does Spokeo guarantee data accuracy?" listed in its Frequently Asked Questions page states only the following, which notably fails to provide any guarantee:

> Spokeo organizes data from more than 50 types of sources. We are working to ensure that we're getting data from the best possible sources. We look for redundancy with respect to the information we get so we can test accuracy against it.

Spokeo's legal troubles related to the accuracy of its search results have continued after its settlement with the United States. A federal appeals court recently allowed to proceed a proposed class action challenging Spokeo's failure to "follow reasonable procedures to assure maximum possible accuracy" of the information contained in its reports.[9] In that case, the plaintiff alleges that Spokeo published false data about him, including his age, marital status, wealth, education, and a photo of someone else purported to be him, which hurt his employment prospects at a time when he was out of work.

---

[7] Faughnder, Ryan. "Spokeo settles FTC allegations of illegal sale of personal data," *Los Angeles Times* (June 13, 2012), *available at* http://articles.latimes.com/2012/jun/13/business/la-fi-0613-spokeo-20120613; *see* Complaint, *United States of America v. Spokeo, Inc.*, No. 2:12-cv-5001 (C.D. Cal. filed on June 7, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeocmpt.pdf.

[8] *Id.*; Mullin, Joe, *supra* n. 2; Dave, Paresh. "Redesigned Spokeo now focuses on reconnecting old pals," *Los Angeles Times* (Aug. 14, 2013), *available at* http://articles.latimes.com/2013/aug/14/business/la-fi-tn-spokeo-focuses-on-reconnecting-old-pals-20130813.

[9] *Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017), *available at* http://cdn.ca9.uscourts.gov/datastore/opinions/2017/08/15/11-56843.pdf.

B. ***Spokeo for Law Enforcement* builds on Spokeo's controversial people search engine by using a proprietary algorithm to collect and analyze data for law enforcement agencies.**

Notwithstanding its history of legal problems, Spokeo recently announced the creation of *Spokeo for Law Enforcement*, a product specifically sold to law enforcement agencies.[10] Spokeo touts that its service connects police investigators "to over 12 billion recordings linking traditional public records with social media," and allows them "fast and easy access to social media data [that] helps officials better track down, monitor and contact individuals."[11]

Public representations by Spokeo raise significant questions about how this software functions. During Spokeo Vice President Aaron Taylor's presentation to the City's Public Safety Commission, Spokeo claimed that it maintains 12 billion records within 300 million people profiles, collected from public sources and over 95 social media platforms.[12] To access this data, Spokeo maintains "proprietary merge technology" allowing it "to process over 12 billion records in less than 18 hours."[13] Although Spokeo's press release announcing the law enforcement tool is short on details, its presentation to the Public Safety Commission suggests that its technology can be used for "behavioral" analyses of individuals' public records and social media activity in ways that it claims will assist the Pasadena Police Department.[14] Pasadena residents deserve to know how this software will function, including whether the software will draw conclusions about Pasadena residents based on proprietary algorithms and privately maintained databases.

II.   The City of Pasadena's interest in *Spokeo for Law Enforcement* raises serious concerns about the privacy and civil liberties of members of the public.

Based on representations made by Chief Sanchez and Manager Mermell, it appears that the City of Pasadena has already committed to a contract with Spokeo for its *Spokeo for Law Enforcement* service. The City previously entered into an agreement for a trial use of the service without seriously considering the privacy risks it raises, without meaningful public debate, and without developing any necessary policies and procedures to limit the potential for its abuse. The City is now prepared to enter into a longer term engagement with Spokeo for this service.

For the reasons set forth below, and as indicated in our August 14 letter, ACLU SoCal has serious concerns about the use of Spokeo's software programs in a law enforcement setting.

---

[10] Press Release, "Spokeo Introduces Investigative Tool for Law Enforcement," Spokeo (July 11, 2017; last edited Aug. 16, 2017), *https://www.spokeo.com/compass/spokeo-introduces-investigative-tool-law-enforcement*.

[11] *Id.*

[12] City of Pasadena Public Safety Committee Regular Meeting Agenda, at 8 (Aug. 16, 2017), *available at* http://ww5.cityofpasadena.net/commissions/wp-content/uploads/sites/28/2017/08/2017-08-16-Public-Safety-Committee-Regular-Meeting.pdf.

[13] *Id.* at 8.

[14] *Id.* at 9–11.

A. **Spokeo's law enforcement service implicates the California Constitution's right to privacy.**

Spokeo's collection and analysis of broad swaths of information and social media data for law enforcement purposes abridges the public's right to privacy enshrined in Article I, Section 1 of the California Constitution. The California constitutional right to privacy "prevents government and business interests from [1] collecting and stockpiling unnecessary information about us and from [2] misusing information gathered for one purpose in order to serve other purposes or to embarrass us." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal.4th 1, 35–36 (1994). The California Supreme Court's description of what the constitutional protection for privacy prohibits perfectly summarizes Spokeo's law enforcement product: the aggregation of disparate public records combined with data from the far reaches of the internet meant to provide policing tools about individuals and their behaviors.

While people understand that some records about them are publicly available, nobody assumes that their real estate records, divorce decrees, consumer protection records, and voter registration preferences would be used to build profiles for police officers to investigate or track them without reason to believe they have committed any crime. The aggregation of that data, coupled with any type of behavioral analysis of that data, works a serious violation of individuals' constitutionally protected right to privacy. Doing so infringes on individuals' expectations of privacy and raises serious questions about the service's legality under the California Constitution.

B. **Spokeo's history of inaccuracy and refusal to guarantee the veracity of its records should invalidate its services for law enforcement use.**

Spokeo's "people search engine" has been the subject of repeated controversy for its failure to provide accurate data for the individuals it profiles, resulting in class action lawsuits and government fines. Spokeo refuses to back the accuracy of these records, notwithstanding its claim to providing law enforcement with a valuable investigative tool.

The Federal Trade Commission fined Spokeo for failing to adequately warn users that the information it provides cannot legally be used to determine eligibility for credit, insurance, employment, or housing, and for failing to follow reasonable procedures for determining the accuracy of its database. But if Spokeo's data lacks sufficient reliability to be used by prospective employers, creditors, insurers, or landlords, it certainly lacks adequate reliability for criminal investigations and police operations. In the hands of a police department, inaccurate data can result in grievous error and serious harm. Bad information could lead police to subject Pasadena residents to baseless and unnecessary surveillance, searches, detentions, and arrests — with the embarrassment and risk of physical force that go along with all law enforcement actions.

Indeed, we conducted own investigation and quickly revealed Spokeo's inaccuracy. We utilized Spokeo's main "people search engine" to look up Larry D'Addario, member of the ACLU's

Pasadena-Foothills Chapter, by his first and last name. Although his name is uncommon, Spokeo's service found 16 individuals with his name in 10 states, including four in California and two in Pasadena. Both of the Pasadena hits clearly refer to Mr. D'Addario, as the results match his middle initial, previous cities of residence, and names of some relatives. But one profile lists an age that is off by nineteen years, and also reports that he utilizes several "aliases," none of which he has ever used. Mr. D'Addario is not alone. In one poll from 2011, Fox News found 10 out of 15 users found inaccuracies in Spokeo's reports, with three stating that their profiles were "mostly inaccurate."[15]

Spokeo's opaque opt-out procedures for individuals' data also concern us, since Spokeo does not clearly provide a mechanism for individuals to opt-out of its *Spokeo for Law Enforcement* service.

Spokeo's history of inaccuracies and its own refusal to guarantee the reliability of its data should disqualify it from use by the Pasadena Police Department.

> **C.   Spokeo keeps its data analysis algorithm secret without subject to public scrutiny.**

Spokeo promises that its law enforcement services will meld public records with troves of public social media data using proprietary software apparently designed to analyze, or facilitate the analysis of, individual behavior. This poses serious potential problems.

As an initial matter, Spokeo's descriptions simply do not clarify what kind of analysis its product actually performs. Does it use the social media and other data it collects to guess who a person might know? Who might be involved in criminal activity? How best to deploy investigative resources? Although predictions made by a computer may appear neutral and objective, they are not infallible. Spokeo's assumptions about the relevance of particular information governs how the service collects and analyzes that information, yet it shields those assumptions from public scrutiny. The public needs to know what kind of analysis Spokeo's software performs in order to understand the risks involved in allowing the Pasadena Police Department to use it.

The City and Spokeo have been equally silent on whether and how the software performs behavioral analysis. Here, a private company—not the Pasadena Police Department, the City Council, or members of the public—decides how to interpret all the collected data and convert it to reports the Department may find useful. What kinds of information does Spokeo's algorithm favor? What does it ignore? How does it weigh individuals' race, political activity, or social connections? The method the software uses to analyze the data relies on the biases and assumptions of Spokeo's creators to inform how it treats these questions.

---

[15] Brandon, John. "Spokeo a Growing Threat to Internet Privacy, Cyber Security Experts Warn," Fox News (Jan. 19, 2011), *available at* http://www.foxnews.com/tech/2011/01/19/spokeo-cyber-security-warn-threat-privacy.html#content.

Even aside from Spokeo's algorithmic assumptions, the data itself may confirm long-standing biases of police officers. For instance, an individual's residence in a high-crime neighborhood should not be weighed as a factor in determining the individual's propensity for committing a crime, since that fact may only be indicative of law enforcement's overpolicing of that neighborhood rather than any disposition of its residents to committing more crimes than average. That individual may have more contacts with law enforcement than an average resident, but only because of increased police activity rather than a propensity for criminality. Without an adequate and open-source investigation into how Spokeo collects and interprets its source data, the Pasadena Police Department runs the serious risk of characterizing as "objective" conclusions drawn by Spokeo based on distorted data about the communities it collects information about. This is to speak nothing of the inherent risk of errors, or "bugs," in the software, an inevitable characteristic of complex computer code that characterizes analytics software.

ACLU SoCal's concerns about Spokeo's proprietary technology by the Pasadena Police Department come as city leaders, privacy organizations, and members of the public increasingly oppose the privatization of policing functions and the deployment of secret data analytics technologies for law enforcement purposes. The example of the City of Fresno's rejection of a policing technology secretly deployed by the Fresno Police Department called *Beware* exemplifies this trend. Without advanced public notice, the Fresno Police Department retained *Beware*, developed by Intrado, Inc. (now called West Corporation), a software technology similar to *Spokeo for Law Enforcement* that collects publically available records and social media data of individuals and feeds that information into a secret algorithm designed to identify the person's "threat score" on a three-part green, yellow, and red color scale.[16] This form of predictive analysis of individuals yielded problematic results based on innocuous (and potentially sensitive) private data. For instance, *Beware* marked a Fresno City councilmember's address as "yellow" (and therefore deserving of extra scrutiny by the police) likely because of the criminal history of a prior tenant, even though the program lacked any basis to flag the councilmember himself.[17] *Beware* also raised one individual's threat score because she tweeted about a card game called "Rage," a word that likely triggered scrutiny of the program.[18] The City eventually halted the use of the program following opposition from community leaders and the ACLU who raised much of the same concerns identified in this letter.[19]

---

[16] Jouvela, Justin. "The new way police are surveilling you: Calculating your threat 'score'", Washington Post (Jan. 10, 2016), *available at* https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.

[17] *Id.*

[18] *Id.*

[19] Sheehan, Tim. "Fresno council halts purchase of data software wanted by the police," Fresno Bee (March 31, 2016), *available at* http://www.fresnobee.com/news/local/article69337677.html.

ACLU
AMERICAN CIVIL LIBERTIES UNION
of SOUTHERN CALIFORNIA
FOUNDATION

LIBERTY | JUSTICE | EQUALITY

The lessons learned from Fresno's experiment with proprietary law enforcement tools must inform the Pasadena City Council and the Pasadena Police Department's consideration of Spokeo's software. The California Constitution enshrines Pasadena residents' right to inspect the *Spokeo for Law Enforcement* service: "The people have the right of access to information concerning the conduct of the people's business." Cal. Const., Art. I, § 3, subd.(b)(1). "[R]ecords related to public business are subject to disclosure if they are in an agency's actual *or constructive* possession." *City of San Jose v. Superior Court*, 2 Cal. 5th 608, 623 (2017). This includes the underlying data and source code of Spokeo's system, which now constitute part of the City of Pasadena's public business. The City's privatization of its investigative responsibilities through the retention of Spokeo risks sowing serious public doubt about how the department conducts its work. The public and city officials should have the opportunity to scrutinize Spokeo's software, including any algorithms and decision-making processes that may affect a member of the public.

D. The City has not offered the public a strong case for why it needs Spokeo's service.

While Spokeo's service poses potentially serious risks of misguided police action and privacy violations, neither the City nor the Police Department have offered any persuasive reasons that its service would significantly benefit public safety. The City should not contract with Spokeo for its data collection and analysis service unless the benefits significantly outweigh the risks to privacy and safety, and unless it conducts a pre-acquisition study of the service and a critical look at the impacts it may have on the public and the police department's job duties. It is the bare minimum requirement that local leaders, stakeholders, and members of the public thoroughly consider the benefits and cons of powerful law enforcement tools and make specific findings of fact justifying their use *before* deploying them. The City has not done so for Spokeo's service.

E. Lack of policies and procedures governing the use of Spokeo creates strong likelihood for abuse.

Finally, the public debate over the *Spokeo for Law Enforcement* service should also be informed by a set of policies and procedures designed to limit how law enforcement officers can use the service. Given the broad scope of the data available to Spokeo, the City of Pasadena must not acquire this service without developing strict policies and procedures governing the circumstances when Spokeo's service may be used, who has access to the service, what level of suspicion is required to use the service to view data on an individual, how records gathered from the service are collected, whether the data can be stored by the City, how the accuracy of the data can be verified, and procedures for deleting any Spokeo data collected by the City. Setting aside the legality and effectiveness of the service, the City and its Police Department should not engage Spokeo without a comprehensive set of policies, procedures, and trainings that address these fundamental questions.

Considering these concerns, ACLU SoCal urges the City of Pasadena and the Pasadena Police Department to cease any ongoing relationship with Spokeo, and to develop a plan for an open,

public debate about the efficacy of Spokeo's products given the dubious legality of the service and the grave concern for individual privacy rights that arises from its use.

III.   California Public Records Act request

With these concerns mind, we request under the California Public Records Act, California Government Code section 6250 et seq., records[20] regarding Spokeo's *Spokeo for Law Enforcement* service and regarding any other Spokeo search engine and software designed to access information from public records and social media services,[21] as follows:

Please provide copies of all records mentioning or referencing *Spokeo for Law Enforcement* or the trial, acquisition, installation, or use of any Spokeo services by the Pasadena Police Department, including but not limited to: grant applications, budget requests, loans, donations, or other funding records; meeting agenda, public notices, and communications to and from any City employee concerning any Spokeo services; records referencing the purchase, acquisition, subscription to, or payment for any Spokeo services; and all product manuals, guidance, policies, or training materials governing the features of and uses of any Spokeo services.

If you determine that some but not all the information is exempt from disclosure and that you intend to withhold it, we ask that you redact it for the time being and make the remaining responsive records available as requested. In any event, please provide a signed notification citing the legal authorities on which you rely if you determine that any or all of the information is exempt and will not be disclosed. If we can provide any clarification that will help expedite your attention to our request, please contact Mohammad Tajsar at (213) 977-9500, ext. 268.

Because this request is on a matter of public concern, we request a fee waiver. We also request that documents be provided in electronic format if possible. Doing so would eliminate the need to copy the materials and provides another basis for our requested fee waiver. If, however, such a waiver is denied, we will reimburse you for the reasonable cost of copying. Please inform us in advance if the cost will be greater than $50.
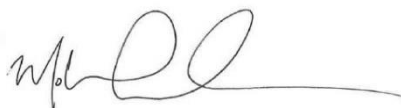
---

[20] Throughout this request, the term "records" includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas, meeting minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, or other similar materials.

[21] When referencing *Spokeo for Law Enforcement* or "any other Spokeo service," this request includes software that enables the monitoring, searching, collection, or analysis of public records or user-generated content located on social media services, including Spokeo's flagship "people search engine" as well as the *Spokeo for Law Enforcement Service*. Examples of such social media services include but are not limited to Facebook, Instagram, Twitter, Google Plus, Pinterest, YikYak, Reddit, SnapChat, and MySpace. Examples of public records include court records, real estate records, voter registration information, marketing surveys, data lawfully sold by data brokers, or consumer credit information.

According to the California Public Records Act (California Government Code § 6253(c)), a response is required within 10 days. Thank you for your prompt attention to this matter. Please furnish all applicable records to us at mtajsar@aclusocal.org if in electronic format or, if in physical form, at 1313 W. 8th St. Suite 200, Los Angeles, CA 90017.

Sincerely,

Mohammad Tajsar
Staff Attorney
ACLU of Southern California

CC: Councilmember & Vice Mayor John J. Kennedy
Councilmember Tyron Hampton
Councilmember Margaret McAustin
Councilmember Gene Masuda
Councilmember Victor M. Gordo
Councilmember Steve Madison
Councilmember Andy Wilson