2019

Constraining Big Brother: The Legal Deficiencies Surrounding Chicago’s Use of the Strategic Subject List

Aaron Tucek

Follow this and additional works at: https://chicagounbound.uchicago.edu/uclf

Recommended Citation

This Comment is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized editor of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
Constraining Big Brother: The Legal Deficiencies Surrounding Chicago’s Use of the Strategic Subject List

Aaron Tucek†

I. INTRODUCTION

In August 2013, the Chicago Tribune ran a story describing the consequences of a new predictive analysis strategy used by the Chicago Police Department (CPD) to prevent violence.1 The predictive strategy it describes feels almost Kafkaesque—unknown government analysts use a mysterious computer program to estimate the risk someone will be involved in violence, then send in police officers to surprise that unsuspecting person and threaten them with consequences if they do not change their ways:

Robert McDaniel was puzzled when the Chicago police commander dropped by his West Side home unannounced last month. The visit was cordial, but Barbara West’s message was clear: Don’t commit any more crimes or face the consequences. . . . McDaniel, who has multiple arrests on suspicion of minor offenses but only one misdemeanor conviction, learned to his surprise that he had made the so-called “heat list” with more than 400 others across the city who have been deemed by the department to be most prone to violence — either as a perpetrator or victim. . . . Interviewed at his Austin home, McDaniel said he was offended at being singled out by West, commander of the Austin police district. All the attention made him nervous because his neighbors noticed, leading them, he

† B.A. 2015, Emory University; J.D. Candidate 2019, The University of Chicago Law School. Many thanks to Professor Aziz Huq for his insightful feedback and helpful critiques. Thank you as well to The University of Chicago Legal Forum for the opportunity to develop this research and the tireless editorial support.

feared, to wonder if he was a police snitch. Two officers waited outside on the porch while the commander and a criminal justice expert spoke to McDaniel in his home. . . . A 17-year-old girl was shocked to learn she was among a handful of women on the list.²

The new predictive strategy described by the Chicago Tribune was an early iteration of the Strategic Subject List (SSL). The SSL represents Chicago’s contribution to the cutting edge of modern law enforcement: predictive policing. If this early usage of the program is disconcerting, its expansion in the years since is shocking: as of 2016, the Chicago Police Department used the SSL to monitor nearly 400,000 Chicago residents.³

This Comment examines the legal implications of such an expansive and intrusive regime of predictive analytics. It first describes the background of predictive policing in Chicago by summarizing the publicly available knowledge regarding the SSL. It then examines the SSL using three different legal frameworks: the Fourth Amendment, the Due Process Clause of the Fourteenth Amendment, and the Illinois Civil Rights Act.

This analysis reveals several constitutional and statutory defects in the current usage of the SSL. Chicago police almost certainly cannot use the SSL as a basis for reasonable suspicion or probable cause. Placing someone on the SSL may constitute an unreasonable search in violation of the Fourth Amendment, depending upon how current doctrine continues to evolve. Placing someone on the SSL also violates the Fourteenth Amendment by depriving that person of protected liberty interests in information privacy and avoiding stigma without due process of law. Finally, by disproportionately burdening Chicago’s African-American and Latino communities, current usage of the SSL results in a racially disparate impact in violation of the Illinois Civil Rights Act. In light of these numerous deficiencies, the City of Chicago should at a minimum provide individuals on the SSL with notice and the opportunity to be heard; the city should also reform the program to eliminate its racially disparate impact. However, disbanding the SSL program altogether would best protect the substantial privacy interests of Chicago residents.

² Id.
II. PREDICTIVE POLICING IN CHICAGO

This Comment seeks to answer an important question for Chicago residents: is the Chicago Police Department using the SSL in a manner consistent with the rights of the city’s citizenry? The first step towards answering this question requires understanding the factual circumstances surrounding Chicago’s usage of the SSL. Consequently, this section endeavors to explain the concept of predictive policing and its application in the City of Chicago, the relevant technical aspects of the SSL, and the manner in which Chicago police use the SSL.

A. Predictive Policing Generally

Although the term “predictive policing” encompasses a broad umbrella of police strategies, it primarily characterizes any approach that seeks to utilize modern computing power to better prevent crime. As the National Institute of Justice explains:

Predictive policing tries to harness the power of information, geospatial technologies and evidence-based intervention models to reduce crime and improve public safety. This two-pronged approach—applying advanced analytics to various data sets, in conjunction with intervention models — can move law enforcement from reacting to crimes into the realm of predicting what and where something is likely to happen and deploying resources accordingly.\(^4\)

Thus, unlike traditional policing strategies that react to crime, predictive policing seeks to move the focus to proactively preventing crime.\(^5\) Such approaches build upon patrol officers’ local knowledge of their beats\(^6\) and the “CompStat” systems developed in the 1990s that popularized the use of crime data in policing decisions.\(^7\) Predictive policing

---


\(^5\) Id.


\(^7\) See Elizabeth E. Joh, Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35, 43–44 (2014) ([the CompStat system involved] weekly meetings at the N.Y.P.D. headquarters at which a revolving group of commanding officers around the city gave accountings of themselves for the recent crime data collected in their precincts. By evaluating performance by the rise or fall of crime data within their precincts, CompStat meetings forced accountability upon commanding officers. Such data-driven policing spread to other departments around the United States when crime rates began to fall dramatically within New York City, a result the police attributed to its reliance upon CompStat, along with the adoption of “broken windows” policing and aggressive stop and frisk tactics. CompStat and similar programs inspired...
innovates over these earlier methods by using of computer algorithms to analyze large datasets. That said, predictive policing is not limited to describing “the application of computer modeling to historical crime data to predict future criminal activity.” Predictive policing is best understood as “any crime fighting approach that includes a reliance on information technology (usually crime mapping data and analysis), criminology theory, predictive algorithms, and the use of this data to improve crime suppression on the streets.”

There are two general categories of predictive policing: place-based and person-based. The place-based method takes a “heat map” approach, which involves “drawing on crime data, geography, weather information, consumer financial records, property records, and other data to predict where and when future crime is most likely to occur.” By contrast, the person-based method seeks to predict who will be involved in future criminality. This technique can involve a “social network analysis,” in which a computer program seeks to “identify likely criminality based on the role an individual plays within a social network,” as well as compiling lists of “individuals [police] predict will commit crimes in the future or are involved in ongoing criminal activity but have not yet been caught.” Although multiple jurisdictions have experimented with both types of predictive policing strategies, place-based strategies are more common.

---

8 See, e.g., id. at 44 (“The innovation of predictive policing is the application of artificial intelligence to such large data sets.”).
9 Id. at 42.
10 See Ferguson, supra note 6, at 265.
13 Polansky & Fradella, supra note 11, at 257.
15 Joh, supra note 7, at 46.
16 Ferguson, supra note 14, at 373.
17 See Ferguson, supra note 6, at 268–69 (“The Los Angeles and Santa Cruz Police Departments may be ahead of other cities in testing the predictive policing model, but they are by no means the only law enforcement agencies using the technique. Jurisdictions as diverse as Palm Beach County, Florida; Memphis, Tennessee; Chicago, Illinois; Minneapolis, Minnesota; and Dallas, Texas, are testing predictive policing tactics.”); Ferguson, supra note 14, at 373 (identifying Charlotte-Mecklenburg, North Carolina as a jurisdiction which uses the “bad guy list” method).
18 See Polansky & Fradella, supra note 11, at 257–58.
The Chicago Police Department utilizes both place-based and person-based predictive strategies. In the place-based category, Chicago police use technologies known as “HunchLab” and “ShotSpotter.” HunchLab “combines crime data with factors including the location of local businesses, the weather, and socioeconomic information to forecast where crime might occur,” while ShotSpotter “uses sensors to locate the source of gunshots.” As part of a pilot program aimed to deploy police resources more effectively and reduce response times, these technologies are currently operated out of “Strategic Decision Support Centers” in six districts. The Police Department credits these support centers, which operate as “hyperlocal intelligence hubs . . . support[ing] a predictive deployment of officers,” as directly contributing to a decline in violence in the districts where they are operational.

Within this person-based category lies this Comment’s primary focus, the SSL, which Chicago police have used since 2012.

B. The Strategic Subject List

The Chicago Police Department describes the SSL as a tool used “to rank individuals with a criminal record according to their probability of being involved in a shooting or murder, either as a victim or an offender. . . .” The algorithm involved, based initially on work done by Yale sociologist Andrew Papachristos, considers a variety of factors mostly related to a person’s criminal history. Although the precise factors used have evolved in subsequent iterations of the software, the most recent publicly available version of the SSL took

---


20 Id.


22 Id.

23 See McLaughlin, supra note 19.


26 See Gorner, supra note 1.

27 SPEC. ORDER S09-11, supra note 25.

28 See Dumke & Main, supra note 3; OFFICE OF NEWS AFFAIRS, CHI. POLICE DEPT., CPD WELCOMES THE OPPORTUNITY TO COMMENT ON RECENTLY PUBLISHED RAND REVIEW (2016), http://4abpn833c0nr1zvwp7447f2b.wpengine.netdna-cdn.com/wp-content/uploads/2016/08/RAND

Using these factors, the algorithm calculates “a score from 1 to 500, with higher scores representing greater risk for future involvement with a shooting or murder.”

Chicago police have not been forthcoming regarding the weight which the algorithm gives each of these eight factors when calculating a final score. Nevertheless, by using linear regression analysis, the New York Times was able to estimate the likely impact of each factor. Journalists concluded that age and victimhood were the two elements with the greatest impact on the SSL risk score:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Marginal Increase in Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of assault or battery incidents (as victim)</td>
<td>+34</td>
</tr>
<tr>
<td>No. of shooting incidents (as victim)</td>
<td>+17</td>
</tr>
<tr>
<td>No. of arrests for violent offenses</td>
<td>+15</td>
</tr>
<tr>
<td>Trend in criminal activity</td>
<td>+14</td>
</tr>
<tr>
<td>No. of unlawful use of weapon arrests</td>
<td>+12</td>
</tr>
<tr>
<td>No. of narcotics arrests</td>
<td>+5</td>
</tr>
<tr>
<td>Gang affiliation</td>
<td>+4</td>
</tr>
<tr>
<td>Age (per decade)</td>
<td>−41</td>
</tr>
</tbody>
</table>


See Asher & Arthur, supra note 32 (explaining that “[b]ecause the department didn’t release all the information that the algorithm uses, our estimates of the significance of each characteristic are only approximate. But using what was available to us, we could predict risk score very accurately, suggesting that we are capturing much of the important information that goes into the algorithm.”).
However, police have acknowledged that the algorithm has changed since the public release of this data: the program no longer considers gang membership, and less weight is now given to gun and drug arrests. Unless police have added additional factors that have not been made public, these changes suggest the current algorithm relies even more heavily upon victimhood and age.

Age is the only demographic category included in the risk score calculations. Police describe the algorithm as “not us[ing] any information about where the person lives, or race or gender, only the pattern of criminal activity.” That said, the database includes information on gender, race, residency, and the location of most recent arrest. And the police statement that the SSL risk score reflects only “the pattern of criminal activity” is not strictly accurate. If the New York Times estimates are correct, then the inclusion of the age variable “[p]ractically . . . limits the list to young people: No one older than 30 falls within the highest-risk category with a score at or above 480.” Furthermore, if victim experiences have the next largest impact, then each risk score would seem to reflect the criminal behavior of others more than that of the individual to which the score is given. Finally, the extent to which the data captures “criminal activity” is questionable. The SSL calculations use data on arrests, not convictions. Given the presumption of innocence, arrest data is at best, an imperfect measure of criminal activity.

The Chicago Police Department has also been misleading about the size of the SSL. Early statements by police officials to the media suggested that the list contained only about 1,400 names. Yet a lawsuit by the Chicago Sun Times, which forced the Police Department to disclose information regarding the SSL to the public, revealed that the list “includes more than 398,000 entries—encompassing everyone who

---

35 See id.; Dumke & Main, supra note 28.
36 See Dumke & Main, supra note 28.
37 SPEC. ORDER S09-11, supra note 25.
38 See STRATEGIC SUBJECT LIST, supra note 29.
39 SPEC. ORDER S09-11, supra note 25.
40 See Asher & Arthur, supra note 32.
41 See STRATEGIC SUBJECT LIST, supra note 29; CPD WELCOMES THE OPPORTUNITY, supra note 28.
has been arrested and fingerprinted in Chicago since 2013."\textsuperscript{43} Police officials have since argued that the 1,400 figure referred only to “individuals who score 480+ which are the highest risk to become a suspect or victim of gun violence.”\textsuperscript{44} However, this statement is not accurate per the publicly available data. In this data, only 285 people have a risk score of 480 or higher.\textsuperscript{45} Reaching the 1,400 figure requires looking at all those who have scores of 429 and above.\textsuperscript{46} While it is true that people in this group were disproportionately likely to be involved in a shooting or murder, the \textit{New York Times} found “that [this] disproportionate share amounted to less than 20 percent of the total gun violence in Chicago in 2016.”\textsuperscript{47} Rather, the majority of gun violence involved individuals with risk scores in the range from 300-420.\textsuperscript{48}

Furthermore, the list mainly tracks men of color. Although the algorithm does not consider race in calculating risk scores, this does not mean that the actual distribution of individuals on the list is blind to race. African-Americans account for more than half of the individuals on the list.\textsuperscript{49} Furthermore, \textit{Chicago Magazine} reports that 56 percent of black men aged 20-29 and 23% of Latino men aged 20-29 residing in Chicago have an SSL score, compared to only 6% of white men in the same age range.\textsuperscript{50} Additionally, the \textit{Chicago Sun Times} reports that “the vast majority of people with the highest score—85 percent—were African-American men.”\textsuperscript{51} Considering this demographical data in light of the importance of age in determining risk score discussed above, the SSL serves largely to identify young African-American men as being particularly at risk for violence.

C. Uses of the Strategic Subject List

The Chicago Police Department uses the SSL for two purposes: intervention and enforcement. The intervention prong proceeds through the use of a “Custom Notifications” system. Unfortunately,
very little is known publicly about how the SSL factors into CPD enforcement activities. Chicago police have largely refused to disclose any information regarding how they use the list. Nevertheless, enough information is available to draw reasonable conjectures as to how the data is being employed.

1. Intervention

One use of the SSL is to provide social services to those particularly at risk of violence through a program known as “Custom Notifications.” As Police Department policy explains:

The custom notification will identify those at-risk individuals and reach out to advise them of the risks and consequences of their actions should they engage in criminal conduct. The goal is to ensure the individual is not only informed of the law enforcement consequences for deciding to engage or continue in gun violence, but also of the devastating impact of gun violence within their community. Opportunities for seeking assistance will also be provided during the custom notification. However, it is ultimately the decision of the individual to choose not to engage in criminal activity.

Review of the SSL is a primary tool used by District Intelligence Officers to identify individuals eligible to receive a custom notification. As CPD policy further explains, once an individual is identified, they will be contacted by a “Custom Notifications Team” formed specifically to get through to the individual. This team then delivers a “Custom Notifications Letter” to the identified individual and explains the contents of the letter. According to the Police Department,

The Custom Notification Letter will be used to inform individuals of the arrest, prosecution, and sentencing consequences

---

52 See Kunichoff & Sier, supra note 24 (“[T]here’s very little information available about how police are using the list. Asked to provide details which social services are offered and how, or how the SSL might assist in investigations, city and police officials either declined to comment or referred reporters to other people who could not answer.”).

53 SPEC. ORDER S09-11, supra note 25 (“The SSL model drives a custom notification process that identifies potential criminal actors and victims associated with the continuum of violence”).

54 CHI. POLICE DEPT., SPEC. ORDER S10-05: CUSTOM NOTIFICATIONS IN CHICAGO (2015), http://directives.chicagopolice.org/directives/data/a7a57bf0-1456fa9-bfa14-570a-a2deebf33c56ae59.html [perma.cc/2RA5-456U] [hereinafter SPEC. ORDER S10-05].

55 Id.

56 Id.; Kunichoff & Sier, supra note 24 (“[T]he program sends out police officers, community members, and personal friends to convince an individual (typically gang-affiliated) that they are risking their life or their freedom by being involved in violence.”).

57 SPEC. ORDER S10-05, supra note 54.
they may face if they choose to or continue to engage in public violence. The letter will be specific to the identified individual and incorporate those factors known about the individual inclusive of prior arrests, impact of known associates, and potential sentencing outcomes for future criminal acts.58

Chicago police frequently tout the role the SSL plays in this Custom Notifications process, noting that “police use the list to identify the most at-risk people and reach[] out to community organizations to help them in ‘finding success in life outside of crime.’”59 However, the Custom Notifications process fundamentally remains a law enforcement deterrence tool. Department policy clearly states that “custom notifications serve as notice that law enforcement action will not be random, but rather targeted and specific to the individual, and the failure to follow the clear and consistent message to cease participating in gun violence will have specific and cognizable penalties, as contained within the custom notification letter.”60 During visits by a Custom Notifications team, “the police bluntly warn that the person is on the department’s radar,”61 and make clear that “further criminal activity, even for the most petty offenses, will result in the full force of the law being brought down on them.”62 CPD policy makes clear exactly what “full force of the law” means in such circumstances: “[t]he highest possible charges will be pursued for any individual in the . . . Custom Notification Program.”63

Although inclusion in the Custom Notifications Program can thus result in serious consequences, the small scope of the program limits its impact. As Chicago Magazine reports, “in 2016, 1,024 notifications were attempted, 558 were completed, and only 26 people attended a call-in.”64 Furthermore, in the three years prior to 2016, police attempted only 1,300 custom notifications of individuals with SSL scores.65 Thus, the great majority of individuals on the SSL will not interact with the Custom Notifications program.

58 Id.
59 Ali, supra note 44 (quoting policing spokesman Anthony Guglielmi); see also Kunichoff & Sier, supra note 24; Dumke & Main, supra note 28 (“[police spokesman] Guglielmi says the scores are mostly used by police and outreach workers to warn those at risk they could be headed for catastrophe and to offer help finding jobs and counseling”); Gorner, supra note 1 (“[P]olice extend them an olive branch of sorts, an offer of help obtaining a job or of social services.”).
60 SPEC. ORDER S10-05, supra note 54.
61 Davey, supra note 42.
62 Gorner, supra note 1.
63 SPEC. ORDER S10-05, supra note 54.
64 Kunichoff & Sier, supra note 24.
65 See Davey, supra note 42.
2. Enforcement

Beyond simply delivering Custom Notification, however, Chicago police also use the SSL for enforcement purposes. Although the CPD has told the media that “the SSL is a simply a tool that calculates risk . . . [and] is not used for enforcement,”66 official documents contradict this characterization. The policy directive establishing the SSL unambiguously states that “Department members may use the SSL as an investigative resource.”67 Other documents imply that police officers do indeed use the SSL for investigatory purposes68 and that the Department actively seeks to integrate use of the SSL into mission assignments.69

Although police do likely use the SSL for enforcement purposes, the Department has imposed limits on such use. A person cannot be arrested simply because their name appears on the list.70 Furthermore, “[p]lacement on the SSL is not a factor for consideration of reasonable suspicion or probable cause and a subject’s score will not be included on any case or arrest reporting documentation.”71 Thus, CPD use of the SSL lies somewhere between using it for enforcement and not using it to establish reasonable suspicion.

Publicly available information suggests police strike this balance by using the SSL as a tool to aid in initial phases of investigation and to monitor individuals on the list. The New York Times reports that “[t]he risk scores have been used numerous times to guide large-scale roundups.”72 Furthermore, CPD has hired the University of Chicago Crime Lab to conduct a “[t]otal overhaul of mission assignments to use predictive analytics and SSL on offenders.”73 If the SSL is used in mis-

---

66 Ali, supra note 44.
67 SPEC. ORDER S09-11, supra note 25.
68 CPD WELCOMES THE OPPORTUNITY, supra note 28 (“t]he SSL informs numerous CPD strategies”).
71 SPEC. ORDER S09-11, supra note 25; see also Ali, supra note 44 (“does not establish probable cause for arrest or even questioning”).
72 Asher & Arthur, supra note 32; cf. Kunichoff & Sier, supra note 24 (“CPD has stated that 280 individuals with SSL scores were arrested in four gang raids during a six-month span in 2016”).
73 NCRB APPLICATION, supra note 69.
sion assignments and has guided “large-scale roundups,” but cannot be used for establishing probable cause, then it stands to reason that police use the list to help identify targets of investigation. Unfortunately, the influence of an SSL score on investigatory decisions remains unknown.

Additionally, the SSL likely serves a “monitoring” function. The sheer size of the list, and the fact that it includes “everyone who has been arrested and fingerprinted in Chicago since 2013,” suggests that one purpose behind the SSL is a desire to track every person with whom police have had a prior crime-related interaction. The police statement that “[i]ndividuals only really come on our radar with scores of 250 and above” supports this inference. The statement implies that there is a qualitative difference between how CPD views someone with a score below 250 and how it views someone with a score above 250. Indeed, the choice of phrase, “come on our radar,” suggests that once an individual’s score exceeds 250, police start paying attention to that individual. Furthermore, this threshold is inconsistent with public statements discussed above, which contend that the list seeks only to identify the 1,400 or so people most at risk for gun violence. Quite to the contrary, at least 270,000 individuals have an SSL risk score exceeding 250. Moreover, police can use the SSL to access a host of information regarding every individual on the list, including demographic and identification information and verified social media identities. With easy access to such a wide range of information, it seems likely that police use the SSL to keep track of a wide swath of the city and facilitate criminal investigations of persons on the list.

D. The Need for Legal Analysis

Given this discussion, an evaluation of the constitutional rights implicated by the SSL deserves close examination. A number of factors raise red flags about the SSL, such as the size of the list, the overrepresentation of communities of color, and the algorithm’s focus on age and victimhood. All suggest the concern that the risk score cal-

---

74 Dumke & Main, supra note 28.
75 Id.
76 A score of 250 is the midpoint in the range produced by the SSL algorithm. See supra note 31 and accompanying text. Considering the secrecy surrounding the algorithm, it is not clear if there is any other reason why police use it as their threshold. What is clear is that it functions as a sorting mechanism: crossing this score seems to trigger the possibility for active monitoring by police (as opposed to exclusively passive tracking by the algorithm).
77 See STRATEGIC SUBJECT LIST – DASHBOARD, supra note 45.
78 SPEC. ORDER S09-11, supra note 25.
culated for a given individual stems from arbitrary factors unrelated to that person’s propensity to commit crime. The lack of transparency regarding how the SSL is used in enforcement is even more worrisome. Beyond a mere unwillingness to reveal to the public how police use the SSL, statements by police officials have consistently misstated facts regarding the program. This tendency provides little reason to trust that the sparse public comments made regarding enforcement provide the full story of police activity. Considering Chicago’s long history of abusive police practices,79 and the likelihood that Chicago police use the SSL for investigatory purposes, this secretive practice by the Department merits close legal scrutiny.

III. THE FOURTH AMENDMENT AND THE STRATEGIC SUBJECT LIST

The Fourth Amendment provides the logical starting point for an analysis of the constitutionality of an enforcement-related police practice, as this area of the Constitution deals most directly with law enforcement. The Fourth Amendment provides that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.80

Two Fourth Amendment questions are relevant for the Chicago Police Department’s use of the SSL: First, can the SSL be used as a foundation for probable cause? Second, does the inclusion of an individual onto the SSL itself constitute an unreasonable search? The answer to both questions is likely no. However, the doctrine regarding unreasonable searches is currently in a state of flux. If the Supreme Court commits to the doctrinal change signaled by five justices in United States v. Jones,81 then placement on the SSL may very well fall into the scope of unreasonable searches under the Fourth Amendment.

80 U.S. CONST. amend. IV.
81 565 U.S. 400 (2012).
A. The SSL as a Foundation for Probable Cause or Reasonable Suspicion

The Fourth Amendment requires a finding of probable cause to support the issuance of a warrant, and it imposes a reasonableness requirement for searches and seizures conducted without a warrant. In other words, “to interfere with a person’s Fourth Amendment rights, law enforcement officers must have either probable cause to search or reasonable suspicion to seize an individual.” Probable cause exists when “the facts and circumstances within [the officers’] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed.” Reasonable suspicion exists when “the facts available to the officer at the moment of the seizure or the search warrant a man of reasonable caution in the belief that the action taken was appropriate.” Reasonable suspicion presents a less rigorous standard than probable cause. If the SSL cannot constitutionally provide a basis for reasonable suspicion, it necessarily follows that it cannot provide a basis for probable cause.

The Supreme Court has given further definition to the requirements of reasonable suspicion in two instances. First, the Court has imposed the threshold requirement that investigatory stops “must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity.” Second, the Court has explained that the “man of reasonable caution” test adopted in Terry v. Ohio requires a consideration of the “totality of the circumstances.” Thus, reasonable suspicion depends on both “the content of information possessed by police and its degree of reliability.” This creates a sliding scale—a greater quantity of information from an unreliable

82 U.S. CONST. amend. IV.
83 Ferguson, supra note 6, at 286.
85 Terry v. Ohio, 392 U.S. 1, 21–22 (1968).
86 See Alabama v. White, 496 U.S. 326, 330 (1990) (“Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause.”).
88 392 U.S. at 21–22.
89 White, 496 U.S. at 330.
90 Id.
source or a lower quantity of information from a more reliable source can both establish a reasonable suspicion.\footnote{See id.}

The Supreme Court has offered direction regarding how to assess the reliability of a source. In United States v. Ventresca,\footnote{380 U.S. 102 (1965).} the Court found that “[o]bservations of fellow officers of the Government engaged in a common investigation,” are reliable sources of information.\footnote{Id. at 111.} Furthermore, police officers may consider “relevant characteristics of location,” such as the stop occurring in a “high crime area,” as long as “[a]n individual’s presence in an area of expected criminal activity” does not form the sole basis for reasonable suspicion.\footnote{Illinois v. Wardlow, 528 U.S. 119, 124 (2000).} Finally, the Court found in Florida v. J.L\footnote{529 U.S. 266 (2000).} that anonymous tips given to police may provide a basis for reasonable suspicion if “suitably corroborated [to] exhibit[ ] sufficient indicia of reliability.”\footnote{Id. at 270.} To suitably corroborate a tip, it must provide predictive information against which police can test the anonymous informant’s knowledge or credibility, and simply describing a person’s “readily observable location and appearance” does not meet this standard.\footnote{Id. at 270–72.}

With these precedents in mind, it is unlikely that the SSL could independently establish reasonable suspicion. As an initial matter, the SSL cannot satisfy the temporal element of the reasonable suspicion test. Under Terry, the existence of reasonable suspicion depends upon “the facts available to the officer at the moment of the seizure or search.”\footnote{Terry v. Ohio, 392 U.S. 1, 21–22 (1968) (emphasis added).} The SSL provides no information about any person’s likelihood of engaging in crime at any particular time. Although the List purports to identify people with a greater risk of either being the perpetrator or victim of gun violence, it makes no temporal prediction as to when that violence will occur. As a result, a police officer who sees someone with an SSL score walking down the street would have no reason to believe, based only upon the SSL score, that criminality was present in that moment.

That said, one might argue that the SSL seems most similar to an anonymous tip, in that it offers information about an individual without allowing police the opportunity to have a direct conversation with the source. The use of the SSL, however, could not meet the suitably corroborated standard for anonymous tips as established in Florida v.
While the SSL does provide information particularized to an individual, the information is not predictive in a Fourth Amendment sense. The SSL score represents the level of risk that an individual will be involved in gun violence as either the perpetrator or the victim. As a result, a high-risk score does not mean that a person on the list is likely to commit a crime. Furthermore, the information produced by the SSL is inherently incapable of independent police observation. An individual’s SSL score represents a mathematical estimate of risk calculated by the police. The police create the list. It is exogenous to the person, and thus cannot be corroborated through observation of the individual. Consequently, the SSL almost certainly cannot independently give rise to a reasonable suspicion.

Furthermore, even if one considers use of the SSL as more akin to a “high crime area” analysis, the SSL would likely add no value to the reasonable suspicion calculation. Illinois v. Wardlow permitted officers to consider whether the stop occurred in a “high crime area” because it is a “relevant contextual consideration.” In other words, location is an independent fact about the world that informs police judgment. The SSL, however, is a police creation. It calculates the risk scores in the manner that it does because police tell it to do so. The list cannot inform police judgment in the same way location might because the SSL is itself, already a product of police judgment. At least based upon publicly available information, it appears to reveal no new or independent facts about the world. Or in other words, the SSL thus seems to offer no additional relevant context that might support a finding of reasonable suspicion. If the underlying factors of the SSL would contribute to finding reasonable suspicion in a given situation, then the SSL score does no work. On the other hand, if the underlying factors would not give rise to reasonable suspicion in those circumstances, then they cannot be made to do so by using a fancy algorithm.

As a result, courts would likely exclude the SSL risk score from reasonable suspicion calculations. Alternatively, one can imagine a world where courts permit police to include SSL score as a factor only when the traditional methods of showing reasonable suspicion do all the work in making the determination. Put differently, it is conceivable that courts might permit an SSL score to support a finding of reasonable suspicion if the support it provides is de minimis. In either case, even the use of the SSL as one factor among many likely could

---

99 529 U.S. 266, 270–72 (2000); see also Navarette v. California, 572 U.S. 393 (2014) (finding that an anonymous 911 caller complaining about a possible drunk driver provided sufficient indicia of reliability by contemporaneously identifying a specific vehicle using a channel of communication in which they were unlikely to lie).

100 528 U.S. at 124.
not constitutionally offer any substantive support for reasonable suspicion.

Consequently, police probably cannot constitutionally use the SSL to support a showing of reasonable suspicion. Use of the SSL as the sole source of reasonable suspicion would therefore likely violate the Fourth Amendment prohibition on unreasonable searches and seizures. Use of the SSL as a factor in showing reasonable suspicion would probably also be impermissible. These concerns may explain why CPD policy makes clear that “[p]lacement on the SSL is not a factor for consideration of reasonable suspicion or probable cause and a subject’s score will not be included on any case or arrest reporting documentation.” As long as Chicago police follow this directive, their use of the SSL in investigations likely remains within the boundaries of the Fourth Amendment.

B. The Creation of the SSL as Constituting a Search

The second key Fourth Amendment question is whether the inclusion of an individual on the SSL itself constitutes an unreasonable search. The controlling case in this context is *Katz v. United States*. In *Katz*, the Supreme Court held that the warrantless invasion of areas in which an individual has “a reasonable expectation of privacy” is “presumptively unreasonable.” *Katz* thus presents two questions: First, has the individual “exhibited an actual (subjective) expectation of privacy?” Second, is the expectation “one that society is prepared to recognize as ‘reasonable?’”

In applying this test, the Court in *Katz* described places such as homes, offices, hotel rooms, or telephone booths as areas in which individuals may have a reasonable expectation of privacy. However, such an expectation does not necessarily arise from these areas: “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” The Supreme Court has subsequently elaborated on this “knowing exposure” exception, finding that: facial characteristics, handwriting, and the sounds of voice are not protected by the Fourth Amendment, and fingerprints may not be protected. Additionally, pri-

101 SPEC. ORDER S09-11, supra note 25.
103 Id. at 360–61 (Harlan, J., concurring).
104 Id. at 361 (Harlan, J., concurring).
105 Id.
106 Id. at 359.
107 Id. at 351.
vate information voluntarily revealed to third parties is not protected, including business records,¹¹⁰ the phone numbers a person dials,¹¹¹ and a person’s movement on public thoroughfares.¹¹²

Despite this history, the Supreme Court’s recent decisions in Jones and United States v. Carpenter¹¹³ call into question the continued vitality of the “third-party doctrine” described in the preceding paragraph. In Jones, five justices agreed that “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”¹¹⁴ As Justice Alito explains: “society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.”¹¹⁵ And the Supreme Court in Carpenter explicitly adopted the view that the contours of the third-party doctrine should change to reflect the sweeping capabilities of modern surveillance technology.¹¹⁶ In that case, the Court continued down the path it began to blaze in Jones by holding that using historic cell site data to track a person’s location violates the Fourth Amendment.¹¹⁷

Whether the Court decides to continue moving away from a strict adherence to the third-party doctrine will likely matter for determining whether placement on the SSL constitutes a Fourth Amendment search. Following the traditional application of Katz and the third-party doctrine, placement on the SSL likely does not violate a person’s reasonable expectation of privacy. However, following the updated approach emerging from Jones and Carpenter likely leads to the opposite result.

1. Third-party doctrine analysis

Under the traditional application of the third-party doctrine, “a person has no legitimate expectation of privacy in information he vol-

---

¹¹⁴ 565 U.S. at 415 (Sotomayor, J., concurring); Id. at 430 (Alito, J., dissenting).
¹¹⁵ Id. at 430 (Alito, J., dissenting).
¹¹⁶ Carpenter, 138 S. Ct. at 2219 (“The Government’s position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period but for years and years”).
¹¹⁷ Id. at 2217 (“Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]”).
untarily turns over to third parties.” This rule appears to cover almost all of the information used by the SSL in its calculation of risk score. The publicly available version of the SSL calculates risk scores based on eight factors: “[1] number of times being the victim of a shooting incident, [2] age during the latest arrest, [3] number of times being the victim of aggravated battery or assault, [4] number of prior arrests for violent offenses, [5] gang affiliation, [6] number of prior narcotic arrests, [7] trend in recent criminal activity and [8] number of prior unlawful use of weapon arrests.” The five factors related to arrest (factors 2, 4, and 6–8) involve easily accessible public records. The two factors related to victimhood (factors 1 and 3) must necessarily stem from communication with police, as victims play a crucial role in initiating police investigation. All seven of these factors therefore involve information voluntarily turned over to third parties, bringing it squarely within the confines of third-party doctrine. As for factor five, it seems extremely unlikely any court would find an objectively reasonable expectation of privacy in gang membership. On this account, therefore, placement on the SSL would not invade a reasonable expectation of privacy under Katz.

2. The impact of Jones and Carpenter

However, analyzing placement on the SSL under the more expansive standard suggested by Jones and Carpenter likely leads to the opposite result. As discussed above, the decisive factor for the five concurring and dissenting justices in Jones and the Court in Carpenter was the expansive “degree of intrusion” enabled by the respective technologies in those cases. Likewise, the predictive algorithm used by the SSL enables government intrusion to a similarly worrying degree by using victim status as a factor in calculating risk score and creating an institutionalized machine of long-term surveillance.

First, the use of victim status as a factor in calculating risk scores impermissibly invades a privacy interest. The Carpenter Court establishes that the third-party doctrine “consider[s] the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents.” Crime victims in Illinois are presumed to have a strong expectation of privacy and gen-

---

118 Smith, 442 U.S. at 743–44.
119 STRATEGIC SUBJECT LIST, supra note 29.
121 See, e.g., supra note 117
122 See Jones, 565 U.S. at 430 (Alito, J., dissenting); Carpenter, 138 S. Ct. at 2217–18.
123 Carpenter, 138 S. Ct. at 2219.
erally have their identities protected from public disclosure.\textsuperscript{124} Unlike the limited personal information revealed by pen registers in \textit{Miller} or the negotiable instruments in \textit{Smith},\textsuperscript{125} crime victim status reveals sensitive, intimate information about a person to which the third-party doctrine should not mechanically apply.\textsuperscript{126}

Additionally, when people report that they have been the victim of a crime, they do so in order to summon the coercive power of the state to seek justice on their behalf. By calling the police, crime victims trigger the state’s fundamental obligation to protect its citizens. People do not anticipate that their calls for help could potentially be used years later to identify them as a target for police enforcement. It makes “no meaningful sense” to consider people in a democratic society availing themselves of their right to the state’s protection of “voluntarily assum[ing] the risk” of turning over information for the government to use surveilling them.\textsuperscript{127} On a policy level, this Hobson’s choice would likely incentivize at least some people at the margins to avoid calling the police when they need help—as a result producing a probable net loss in public safety. Just as in \textit{Jones}, where “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable,”\textsuperscript{128} so to do crime victims expect to relinquish some privacy during the investigation and prosecution of the perpetrator. But “the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.”\textsuperscript{129} Victims do not expect that some of the worst days of their lives may be accessed repeatedly by police to potentially target them for criminal investigation in the indefinite future. Placement on the SSL therefore violates a reasonable expectation of privacy.

Furthermore, the SSL’s structure suggests that it facilitates and enables widespread surveillance on an industrial level. This inference begins by considering how the predictive technology behind the SSL must function. For the algorithm to produce meaningful, up-to-date risk scores, the data for each individual on the list must be continually

---

\textsuperscript{124} See, e.g., 5 ILL. COMP. STAT. 140/7(1)(c) (2017) (Exempting from public inspection “[p]ersonal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information”); State Journal-Register v. Univ. of Ill. Springfield, 994 N.E.2d 705, 718–19 (Ill. App. Ct. 2013) (finding that revealing the name of a crime victim would constitute an “unwarranted invasion of personal privacy [which] outweighs the public interest” and exempting such disclosure under 5 ILL. COMP. STAT. 140/7(1)(c)).

\textsuperscript{125} See \textit{Carpenter}, 138 S. Ct. at 2219.

\textsuperscript{126} See \textit{id.} at 2217–19.

\textsuperscript{127} See \textit{id.} at 2220.

\textsuperscript{128} See \textit{Jones}, 565 U.S. at 430 (Alito, J., dissenting).

\textsuperscript{129} \textit{Carpenter}, 138 S. Ct. at 2219.
updated. Thus, the nature of the SSL requires a constant passive monitoring of everyone on the list for changes in relevant variables. On top of this foundation, consider how the list is populated: it includes every person arrested and fingerprinted in the City of Chicago since 2013.\textsuperscript{130} As of the public release of data in July 2016,\textsuperscript{131} the SSL contained 398,000 entries.\textsuperscript{132} The number of individuals on the list has likely grown even higher since this release. Thus, the constant background monitoring involved in maintaining the SSL affects hundreds of thousands of Chicagoans.

Moreover, consider the impact of the risk scores. Police have indicated that they begin paying attention to individuals who have a risk score above 250.\textsuperscript{133} With the 2016 list, this corresponds to approximately 270,000 people.\textsuperscript{134} How police pay attention to this group remains unknown; however, included in the SSL database is a host of demographic, identification, and social media information\textsuperscript{135}—everything police would need to conduct more detailed monitoring and surveillance activities of these individuals. While it is reasonable to assume that police attention continues to increase in parallel with a heightened SSL risk score, the threshold score of 250 must have some meaning for CPD to so specify it. In the absence of more transparency from the City, one can imagine a system where some sort of occasional surveillance begins at this threshold and then increases in frequency and depth as the score increases. The SSL therefore appears to set up a two-tiered system of basic “data maintenance” monitoring and more intensive “criminal enforcement” monitoring. And because no mechanism currently exists to remove a name from the SSL, this two-tiered system of monitoring may occur at the discretion of police for the indefinite future.

Again, just as in Jones, people may reasonably expect “relatively short-term monitoring” by police.\textsuperscript{136} Depending on the reason for their arrest, they may even reasonably expect a greater-than-usual amount of monitoring for some period following their release. But, like Jones, where the “line [at which police behavior became a search] was surely crossed before the 4–week mark;”\textsuperscript{137} so too here, the line is surely crossed before police surveil hundreds of thousands of people for an

---

\textsuperscript{130} See supra note 43 and accompanying text.
\textsuperscript{131} See supra note 29.
\textsuperscript{132} See supra note 43 and accompanying text.
\textsuperscript{133} See supra notes 75–77 and accompanying text.
\textsuperscript{134} Id.
\textsuperscript{135} See supra note 78.
\textsuperscript{136} See Jones, 565 U.S. at 430 (Alito, J., dissenting).
\textsuperscript{137} Id.
indeterminate number of years. The SSL strongly resembles the sweeping and retrospective surveillance the Court worries about in *Carpenter*. Following the logic of *Jones* and *Carpenter*, such police behavior violates a reasonable expectation of privacy.

Although the Chicago Police Department may not use the SSL as a foundation for probable cause or reasonable suspicion, placing individuals on the list may violate the Fourth Amendment depending upon how case law develops. This uncertainty makes relying on the Fourth Amendment to challenge the usage of the SSL unwise. The Supreme Court may back away from *Jones* and *Carpenter* and return to the third-party doctrine. Or the Court may continue to limit the reach of the third-party doctrine in light of modern technological developments, but adopt a test that would still exclude the SSL. Nevertheless, the SSL provides a good argument that the Supreme Court should adopt an expansive rule of the Fourth Amendment that more robustly protects privacy interests.

The SSL represents one of America’s early experiments with predictive policing; as data sciences continue to improve, the quality and intrusive reach of programs like the SSL will continue to grow. Already the SSL involves the continuous monitoring of hundreds of thousands of people for an indefinite period and judges those people in part by peering into their misfortune of being crime victims. Most people would likely view this as a serious breach of privacy, and so too should the law.

### IV. Procedural Due Process Analysis

Although the SSL and other methods of predictive policing clearly deal with law enforcement, thinking of them solely in terms of Fourth Amendment search doctrine ignores the broader implications of this underlying technology. Predictive data aggregations of the type exemplified by the SSL could have uses for many aspects of government, and it is not difficult to imagine a regime in which these sorts of “lists with consequences” impact access to social services. China provides an extreme example of the possibilities—beginning in 2020, the Chinese government will produce trust scores for all citizens by peering deeply into their private lives. People with higher trust scores will be rewarded with a variety of social service and commercial benefits, while

---

138 See *Carpenter*, 138 S. Ct. at 2218.

those with lower scores will see penalties.\textsuperscript{140} While it is nearly impossible to imagine such a pervasive system ever gaining traction in the United States, the China example helps illustrate the need to view the SSL as more than a law enforcement tool. Rather, the SSL should also be viewed as one variety of this broader category of “lists with consequences.”

Considering the SSL from this angle reveals an additional constitutional deficiency: placement on the SSL by the Chicago Police Department likely works a deprivation of liberty without due process of law in violation of the Fourteenth Amendment. To reach this conclusion, this section provides: an overview of procedural due process jurisprudence, examines the application of procedural due process in airline no-flight list cases, and finally, analyzes the SSL under this doctrine.

A. Overview of Procedural Due Process

The Fourteenth Amendment provides that “no state shall . . . deprive any person of life, liberty, or property, without due process of law.”\textsuperscript{141} Constitutionally adequate process minimally requires notice and the opportunity to be heard.\textsuperscript{142} Further determining the precise procedures required in a given situation is a fact-intensive process. As the Supreme Court held in \textit{Mathews v. Eldridge},\textsuperscript{143} due process requires the consideration of three factors:

First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government’s interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.\textsuperscript{144}

When the \textit{Mathews} balance weighs in favor of the government, no additional process is required; however, adequate due process requires additional procedures when the balance weighs toward the individual.

The recent movement of courts to apply \textit{Mathews} balancing in airline no-fly list cases suggests the propriety of using this reasoning in

\textsuperscript{140} \textit{Id.}
\textsuperscript{141} U.S. CONST. amend. XIV., § 1.
\textsuperscript{142} \textit{See}, \textit{e.g.}, \textit{Mullane v. Central Hanover Bank & Trust Co.}, 339 U.S. 306, 313 (1950).
\textsuperscript{143} 424 U.S. 319 (1976).
\textsuperscript{144} \textit{Id.} at 335.
the context of the SSL. In *Latif v. Holder*, the District Court of Oregon held that “the absence of any meaningful procedures to afford Plaintiffs the opportunity to contest their placement on the No-Fly List violates Plaintiffs’ rights to procedural due process.” While courts had dismissed earlier due process challenges to the No-Fly List on jurisdictional grounds, the Ninth and Sixth Circuits led the way in rejecting such reasoning beginning in 2012. With the jurisdictional hurdle cleared, the District Court’s holding in *Latif* spurred the Transportation Security Administration (TSA) to undertake significant reforms. To satisfy the requirements of due process, the *Latif* court required that “the plaintiffs must receive notice of their No Fly List status and a statement of reasons that would enable them to submit responsive evidence.” In reply, the government subsequently pledged to so update its procedures and apply them to a class of individuals beyond the specific plaintiffs in the case. Although difficult questions remain as to the precise requirements of procedural due process in the No Fly List context, *Latif* provides a good example of how procedural due process applies in situations where the government uses a list to track members of the populace.

B. The *Latif v. Holder* Example

As *Latif* demonstrates, the first prong of the *Mathews* balancing test—a private interest affected by placement on the government list—provides the threshold inquiry in procedural due process cases. If placement on the list adversely affects no private liberty or property interest, then the Constitution requires no process. In *Latif*, the Court determined that *Mathews* balancing was appropriate because “Defendants’ inclusion of Plaintiffs on the No–Fly List has deprived Plaintiffs of their constitutionally-protected liberty interests in travel and reputation.” Having made this determination, the *Latif* court then proceeded to weigh these liberty interests against the risk of erroneous
ous deprivation, the probable value of additional safeguards, and the government’s interest, as required by the remaining two prongs of the *Mathews* test.\(^{154}\)

The court found that the TSA’s procedures carried a high risk of erroneous deprivation and that the probable value of additional safeguards was high. Although the government used a “reasonable suspicion” standard to initially place a person on the No-Fly List and had some procedure for challenging one’s inclusion, the court concluded these procedures were insufficient. The procedures carried a high risk of erroneous deprivation because the government refused to tell passengers who were denied boarding and submitted inquiries whether they were on the No-Fly List or why they were placed on the List.\(^{155}\) As a result, the court worried that easily correctable errors would remain unfixed.\(^{156}\) The court further found that “additional procedural safeguards would have significant probative value” because “notice of the reasons for inclusion on the No–Fly List as well as an opportunity to present exculpatory evidence would help ensure the accuracy and completeness of the record . . . [and] would provide aggrieved travelers the opportunity to correct ‘simple factual errors’ with ‘potentially easy, ready, and persuasive explanations.’”\(^{157}\) As a result of these two conclusions, the District Court held that the second *Mathews* factor weighed heavily for the plaintiffs.\(^{158}\)

Next, the court found that significant government interests were at stake. Indeed, the court quickly concluded that “the governmental interests in combating terrorism and protecting classified information are particularly compelling. . . .”\(^{159}\) As a result, the District Court held that the third *Mathews* factor weighed heavily in the government’s favor.\(^{160}\)

After analyzing each factor individually, the *Latif* court finally balanced the *Mathews* factors against one another, ultimately concluding that the Constitution required additional process.\(^{161}\) Although the District Court was sympathetic to the government’s compelling inter-

---

\(^{154}\) *See id.* at 1151–54.

\(^{155}\) *Id.* at 1152–53 (“even simple factual errors may go uncorrected despite potentially easy, ready, and persuasive explanations”).

\(^{156}\) *Id.* at 1153 (quoting Al Haramain Islamic Found., Inc. v. U.S. Dep’t of Treasury, 686 F.3d 965, 982 (9th Cir. 2012)).

\(^{157}\) *Id.* at 1153.

\(^{158}\) *Id.* at 1154.

\(^{159}\) *Id.*

\(^{160}\) *Id.*

\(^{161}\) *See Id.* at 1161–62.
est in national security, the lack of notice to individuals placed on the No-Fly List proved decisive:\footnote{162}{Id. at 1160–61.}

Defendants’ failure to provide any notice of the reasons for Plaintiffs’ placement on the No–Fly List is especially important in light of the low evidentiary standard required to place an individual in the TSDB in the first place. When only an ex parte showing of reasonable suspicion supported by “articulable facts . . . taken together with rational inferences” is necessary to place an individual in the TSDB, it is certainly possible, and probably likely, that “simple factual errors” with “potentially easy, ready, and persuasive explanations” could go uncorrected. \footnote{163}{Id. at 1161.} See \textit{Al Haramain}, 686 F.3d at 982. Thus, without proper notice and an opportunity to be heard, an individual could be doomed to indefinite placement on the No–Fly List. Moreover, there is nothing in the DHS TRIP administrative or judicial-review procedures that remedies this fundamental deficiency. The procedures afforded to Plaintiffs through the DHS TRIP process are wholly ineffective and, therefore, fall short of the “elementary and fundamental requirement of due process” to be afforded “notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present objections.” \footnote{164}{Id. at 1162.} \textit{See Mullane}, 339 U.S. at 314, 70 S.Ct. 652.\footnote{165}{Id. at 1162.}

To remedy this lack of due process, the court ordered the government to provide the plaintiffs “with notice regarding their status on the No–Fly List and the reasons for placement on that List,” such that they could “submit evidence relevant to the reasons for their respective inclusions on the No–Fly List.”\footnote{164}{Id. at 1162.}

C. Application to the Strategic Subject List

Although \textit{Latif} is only a district court case within the Ninth Circuit, it provides a useful lens through which to analyze Chicago’s use of the SSL because of the facial similarity between the No-Fly List and the SSL:

1. Both mechanisms involve government lists of people.

2. Consequences follow for the people on each list.
3. In neither case did the people on the list have notice of their inclusion.

4. The government interest in each situation deals with public safety concerns (national security in *Latif* and reducing violent crime in the SSL context).

5. Finally, the government’s decision to not appeal the *Latif* order and to instead expand their procedural reforms to a class of people beyond the named plaintiffs in the case suggests that the government believed the district court’s ruling was reflective of the likely outcome on appeal.

*Latif* thus provides a good starting point for understanding how a court would approach a procedural due process claim against CPD’s use of the SSL. Although different liberty interests are at stake than in *Latif*, placement on the SSL likely violates at least two protected liberty interests. Furthermore, the second and third *Mathews* factors likely weigh heavily against the government. As a result, the Fourteenth Amendment almost certainly requires individuals placed on the SSL to receive notice and the opportunity to be heard.

1. Deprivation of liberty

Compared to *Latif*, the question of whether placement of a person on the SSL deprives that person of a protected liberty or property interest is less straightforward. The harm resulting from a person’s placement on the No-Fly List is very concrete: the inability to board an airplane. The consequences of an individual’s placement on the SSL are less immediately visible, making identifying the protected liberty interests involved more difficult. Nevertheless, it is clear that the Chicago Police Department’s use of the SSL deprives the people placed on the list of their protected interests in information privacy and avoiding stigma.

a. *Interest in information privacy*

In *Whalen v. Roe*, the Supreme Court described an “individual interest in avoiding disclosure of personal matters.” Although the Supreme Court has not fully developed this constitutional right to information privacy, the Seventh Circuit recognizes this right. In

---

165 *See* Sinnar, *supra* note 147, at 4.
167 *Id.* at 599; *see also* Nixon v. Adm’r of Gen. Servs., 433 U.S. 425, 457 (1977).
168 *See* Nat’l Aeronautics and Space Admin. v. Nelson, 562 U.S. 134, 138 (2011) (“We assume,
The Seventh Circuit, the existence of a privacy interest in information “depends upon whether [there is] a reasonable expectation of privacy in the information.”\textsuperscript{170} This test is virtually identical to that used in \textit{Katz}; as a result, the same considerations apply as in the Fourth Amendment context.\textsuperscript{171} Consequently, the extent of the privacy interest will again depend on the evolution of the ideas expressed by the five concurring and dissenting justices in \textit{Jones}.

However, the test here does go slightly further than in the Fourth Amendment context: because it explicitly focuses on information, the question arises whether an individual on the SSL has a reasonable expectation of privacy in the risk score generated for them? The answer to this question seems to be unambiguously yes. The risk score purports to predict a person’s likelihood to be involved in violent crime. This is incredibly sensitive personal information. As displayed by the Chicago police’s own behavior in using the SSL as an investigative resource, the common inference people draw from learning someone’s risk score is one of criminality. As a person’s risk score increases, the inference correspondingly shifts to one of violent criminality. Any person would want this information to remain as private as possible. Indeed, disclosure of the information may have serious consequences for the individual in their dealings with neighbors, employers, and police. As a result, a person would reasonably expect privacy in their SSL risk score.

Therefore, use of the SSL violates the “individual interest in avoiding disclosure of personal matters.”\textsuperscript{172} Unlike in \textit{Whalen}, where the personal data was heavily fortified and a grand total of only forty-one people had access to the information,\textsuperscript{173} here risk scores are widely accessible by police officers.\textsuperscript{174} Presumably the Chicago police could give access to other government officials or even make risk scores public. But the wide access by police is enough—the ability of any member of the Police Department to look up a risk score, draw a negative inference of the individual based on that risk score, and potentially share that risk score to others in the community, means disclosure is probably fairly widespread. As a result, the use of the SSL invades a constitutionally protected liberty interest.

\textsuperscript{169} See Kimberlin v. U.S. Dep’t of Justice, 788 F.2d 434, 438 (7th Cir. 1986).
\textsuperscript{170} Id.
\textsuperscript{171} See discussion supra Section III.B.
\textsuperscript{172} Id. at 599; see also Nixon, 433 U.S. at 457.
\textsuperscript{174} See SPEC. ORDER S09-11 supra note 67 and accompanying text.
b. Interest in avoiding stigma

In Wisconsin v. Constantineau, the Supreme Court found a protected liberty interest in “a person’s good name, reputation, honor, or integrity.” As the Seventh Circuit has elaborated: this “stigmatic harm . . . must take concrete forms and extend beyond mere reputational interests” for the deprivation of a protected liberty interest to occur. Stigmatic harms flowing from placement on the SSL clearly meet both the “concreteness” and “beyond reputational interests” prongs of this test. Inclusion on the list likely results in: 1) some level of police monitoring, which may include monitoring social media accounts; 2) an increased police assumption that the individual is likely to commit criminal acts (as evidenced by the apparent use of the SSL to inform investigatory decisions); and 3) an increased likelihood that the person will be placed in the Custom Notifications program (which carries with it the threat of severe punishment for any subsequent arrest).

Furthermore, once on the list, the amount of police scrutiny an individual receives depends on factors largely beyond their control, namely: age, victimhood status, past arrests, and even police decisions to change the risk calculation formula. Thus, upon placement on the SSL, an individual may have limited ability to reduce their visibility to police. Moreover, the absence of any mechanism for escaping these consequences effectively turns placement on the SSL into a life sentence. Consequently, the list has the effect of cleaving the city in two: (1) a portion not on the list and presumed to be law-abiding; and (2) the other portion on the SSL and confronted with frequent suspicion by police. Therefore, placement on the SSL results in numerous concrete stigmatic harms, thus depriving persons on the list of a protected liberty interest.

2. Risk of erroneous deprivation and probable value of safeguards

The risk of erroneous deprivation of these liberty interests is very high. Currently, individuals placed on the SSL receive exactly zero process—a person can be placed on the list, have a risk score calculated, and become the target of police monitoring and enforcement behavior with no notice at any point and no opportunity to contest their
presence on the list. Moreover, police use no evidentiary standard to determine who gets placed on the list; to the contrary, any person arrested and fingerprinted in Chicago is entered into the database. At least in *Latif* the government had some evidentiary basis for including a person on the No-Fly List, and some limited procedures existed for challenging one’s inclusion on this list. If the likelihood of erroneous deprivation was high in that case, then it must be even higher in circumstances where not even such limited safeguards exist. Considering the size of the SSL, the list is likely filled with people who pose no risk of involvement in violent crime, regardless of the risk score the algorithm calculates for them.

Additional safeguards would have a great deal of value in reducing this risk. Indeed, given the status quo of no safeguards, adding almost any procedures would reduce the likelihood of error. In particular, procedures that gave individuals notice of their inclusion on the list and some opportunity to contest that inclusion would go a long way. Just as in *Latif*, notice and the opportunity to be heard would provide “the opportunity to correct ‘simple factual errors’ with ‘potentially easy, ready, and persuasive explanations.’” 179 Considering that factors beyond individual control—namely age and victimhood status—heavily drive the algorithmic calculation of risk scores, many people could likely easily and persuasively explain why a concern that they will commit violent crime is unfounded. Because the risk of erroneous deprivation and the probable value of additional safeguards are both so high, the second *Mathews* factor appears to weigh more strongly in favor of a person on the SSL than it did in favor of the *Latif* plaintiffs.

3. Government interest

The government likely has a lesser interest in the SSL context than it did in *Latif*. The government undoubtedly has a valid and compelling interest in reducing violent crime. However, the link between the SSL and crime reduction is much less straightforward than between the No-Fly List and national security. By preventing suspected terrorists from getting on airplanes, the No-Fly List theoretically functions to proximately prevent acts of terror in air travel. The causal link between the SSL and crime reduction is much more attenuated. While the steps that formulate the SSL—creating a dragnet list of every person arrested in the city, developing a predictive algorithm, applying that algorithm to everyone on the list to estimate risk of involvement in a shooting or murder, then using that list to guide inter-

---

vention and enforcement activity—plausibly provides some assistance to the police in their efforts to reduce gun violence, the marginal impact of the SSL on gun violence appears to be much smaller than the marginal impact of the No-Fly List on terrorism. In fact, the only published empirical study of the SSL called into doubt the predictive power of an early version of its algorithm.\textsuperscript{180} As a result, the City’s interest in the SSL is less than the federal government’s interest in the No-Fly List described in \textit{Latif}.

Within the SSL context then, the second \textit{Mathews} factor weighs more heavily toward an individual on the list, and the third \textit{Mathews} factor weighs less heavily toward the government than in \textit{Latif}. Considering how the lack of notice proved decisive for the \textit{Latif} court, a complete lack of any process in the SSL context and a \textit{Mathews} balance less favorable to the government should make this an easy procedural due process case. As the Supreme Court has stated, “[w]here a person’s good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential.”\textsuperscript{181} So too here: the Due Process Clause of the Fourteenth Amendment likely requires Chicago police to provide individuals whose names are placed on the SSL with notice and the opportunity to be heard.

\textbf{V. THE ILLINOIS CIVIL RIGHTS ACT}

In addition to the constitutional concerns posed by the SSL, the Chicago Police Department’s use of the list also raises issues under the Illinois Civil Rights Act. The Act provides that:

No unit of State, county, or local government in Illinois shall: (1) exclude a person from participation in, deny a person the benefits of, or subject a person to discrimination under any program or activity on the grounds of that person’s race, color, national origin, or gender; or (2) utilize criteria or methods of administration that have the effect of subjecting individuals to discrimination because of their race, color, national origin, or gender.\textsuperscript{182}

To state a \textit{prima facie} claim under this statute, “[a] plaintiff must allege that defendant treated the plaintiffs differently because of their

\textsuperscript{180} See Jessica Saunders, et al., \textit{Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago’s Predictive Policing Pilot}, 12 J. EXPERIMENTAL CRIMINOLOGY 347, 347 (2016) (“Individuals on the SSL are not more or less likely to become a victim of a homicide or shooting than the comparison group.”).


\textsuperscript{182} 740 ILL. COMP. STAT. 23/5(a) (2017).
inclusion in an identifiable and constitutionally protected class.”  

Once the plaintiff has made and proved such an allegation, the burden shifts to the City to demonstrate that its policy or practice had “manifest relationship” to a legitimate, non-discriminatory policy objective and was necessary to the attainment of that objective. . . . If the City shows that its actions were justified, then the burden shifts back to Appellants to show ‘a viable alternative means’ was available to achieve the legitimate policy objective without discriminatory effects.  

Importantly, the Illinois Civil Rights Act “does not reference intent of the allegedly discriminatory party.”

The Chicago Police Department’s use of the SSL likely would support a disparate impact claim under the Illinois Civil Rights Act. Young men of color are overrepresented on the list, and large proportions of the African-American and Latino communities in Chicago find themselves included on the SSL. By contrast, only a small proportion of the white community is included on the SSL. In light of the two-tiered monitoring scheme discussed above, the impact of these racial disparities translates into the police having a large amount of surveillance penetration into Chicago’s black and brown communities, while exercising very little corresponding penetration into the city’s white community. This race-based discrepancy in policing looks very similar to that described in Central Austin Neighborhood Association v. City of Chicago. The court in Central Austin denied the City’s motion to dismiss, finding that Chicago’s use of “a method of administering responses to 911 calls that ha[d] the effect of subjecting the residents of police districts populated mostly by African-Americans and Hispanics to longer waiting periods, on average, for responses to 911 calls” sufficiently alleged a violation of the Act. Therefore, just as in Central Austin, the CPD’s use of the SSL likely “utilize[s] criteria or methods of administration that have the effect of subjecting individuals to discrimination because of their race, color, national origin, or gender” in violation of the Illinois Civil Rights Act.

---

185 McFadden, 2006 WL 6284486, at *8.
186 See supra note 49 and accompanying text; Kunichoff & Sier, supra note 24; Dumke & Main, supra note 28.
187 See Kunichoff & Sier, supra note 24.
188 1 N.E.3d at 980.
The Chicago Police Department may respond that use of the SSL has a “manifest relationship” to the “legitimate, non-discriminatory policy objective” of reducing violent crime. However, considering that the SSL is designed to identify people likely to be involved in a violent crime as either the perpetrator or victim, the relationship between risk score and actual propensity to commit violent crime must be attenuated at best. Some scholarship on an early version of the SSL even suggests that the algorithm used may lack predictive power altogether. Given the resulting high likelihood of sweeping up innocent individuals, it seems simply false to say that use of the SSL, regardless of its racially disparate impact, is “necessary to the attainment” of violent crime reduction.

Furthermore, it is easy to imagine many “viable alternative means . . . without discriminatory intent.” For example, the City could hire more homicide detectives to improve its abysmal and historically low murder clearance rate, thereby increasing the deterrence and incapacitation of violent offenders. At any rate, a court need not tell the City exactly how to remedy the racially disparate impact; “the City will retain authority to devise procedures that have no unjustified discriminatory effects.” Thus, separate from the program’s constitutionality, the Chicago Police Department’s use of the SSL likely creates a racially disparate impact in violation of the Illinois Civil Rights Act.

VI. CONCLUSION

This Comment calls into question the legality of the Chicago Police Department’s use of the SSL. The SSL likely cannot be used as a basis for probable cause or reasonable suspicion. Placement on the SSL may itself constitute an unreasonable search under the Fourth Amendment, depending upon whether and how the Supreme Court chooses to limit the third-party doctrine following its decisions in

---

190 Cent. Austin, 1 N.E.3d at 980.
191 See SPEC. ORDER S09-11, supra note 25.
192 See Saunders, et al., supra note 180 at 347 (“Individuals on the SSL are not more or less likely to become a victim of a homicide or shooting than the comparison group”).
193 Cent. Austin, 1 N.E.3d at 980.
194 Id.
196 Cent. Austin, 1 N.E.3d at 983.
United States v. Jones\textsuperscript{197} and Carpenter v. United States\textsuperscript{198} Additionally, even if placement on the SSL does not violate Fourth Amendment rights, the List nevertheless invades the liberty interests in information privacy and avoiding stigma of those placed on it. In light of these deprivations and the complete lack of any protective procedures, the balancing test under Mathews v. Eldridge indicates that current usage of the SSL violates the procedural due process rights of individuals placed on the List\textsuperscript{199} Finally, independent of these constitutional violations, the racially disparate impact of the SSL likely violates the Illinois Civil Rights Act.

These numerous legal deficiencies suggest that cities in general should proceed carefully with the creation of predictive policing technologies such as the SSL. Ideally, courts will expand Fourth Amendment doctrine in a way that recognizes the pervasive threat predictive analytics poses to individual privacy. Even if it does not, the procedural due process analysis conducted herein suggests that individuals placed on such “lists with consequences” by the government must receive notice and the opportunity to be heard. Additionally, the government should ensure that the predictive technology it uses does not impose racially disparate burdens upon marginalized communities.

As for Chicago in particular, this analysis demands serious accountability for the SSL program. The City should vastly increase its transparency about how it uses the SSL so that the public may explore the full extent of the enforcement, its wide-spread surveillance, and its disparate impact on marginalized communities. More importantly, the City should immediately reform the program to provide notice and the opportunity to be heard to all individuals placed on the list, and to eliminate its racially disparate impact. Yet even if these reforms are made, the SSL still will likely invade the privacy interests of thousands of Chicagoans. Therefore, an end to the SSL would best protect the liberty of the people of Chicago. Chicago police have legitimate authority because of the consent of the governed. They are not Big Brother. A secretive government watch-list that facilitates the indefinite surveillance of nearly 400,000 Chicagoans is simply inconsistent with the ideals and laws of a free society.

\textsuperscript{197} 565 U.S. 400 (2012).
\textsuperscript{198} 138 S. Ct. 2206 (2018).
\textsuperscript{199} See 424 U.S. 319, 335 (1976).