# A Political-Economy Analysis of the Provision of Urban Anti-Crime Technologies in a Model With Three Cities

Batabyal, Amitrajeet and Kourtit, Karima and Nijkamp, Peter

Rochester Institute of Technology, Open University, Heerlen, JADS

7 November 2019

# A Political-Economy Analysis of the Provision of Urban Anti-Crime Technologies in a Model with Three Cities[1]

by

**AMITRAJEET A. BATABYAL,[2]**

**KARIMA KOURTIT,[3]**

**and**

**PETER NIJKAMP[4]**

1

For their helpful comments on two previous versions of this paper, we thank the Associate Editor Nazrul Islam, three anonymous reviewers, and participants in the Cities4People International Workshop in the Jheronimus Academy of Data Science (JADS), 's-Hertogenbosch, the Netherlands, in November 2019. In addition, Batabyal acknowledges financial support from the Gosnell endowment at RIT. The usual absolution applies.

2

Department of Economics, Rochester Institute of Technology, 92 Lomb Memorial Drive, Rochester, NY 14623-5604, USA. E-mail: aabgsh@rit.edu

3

Alexandru Ioan Cuza University, Iasi, Romania, Polytecnic University, Ben Guerir, Morocco, Uppsala University, Uppsala, Sweden, Centre for the Future of Places (CFP), KTH Royal Institute of Technology, Stockholm, Sweden, Adam Mickiewicz University, Poznan, Poland, and JADS, Sint Janssingel 92, 5211 DA's-Hertogenbosch, The Netherlands. E-mail: k_kourtit@hotmail.com

4

Alexandru Ioan Cuza University, Iasi, Romania, A. Mickiewicz University, Poznan, Poland, Polytecnic University, Ben Guerir, Morocco, and JADS, Sint Janssingel 92, 5211 DA's-Hertogenbosch, The Netherlands. E-mail: p.nijkamp@jads.nl

# A Political-Economy Analysis of the Provision of Urban Anti-Crime Technologies in a Model with Three Cities


**Abstract**

We use a theoretical political-economy model with three cities and analyze three questions. First, should police in these cities have access to contentious crime fighting technologies such as facial recognition software? We describe a condition involving benefit, cost, and spatial spillover terms which tells us when the police ought to be provided with this technology. Second, if police are to be offered this technology then what are the properties of a policy regime that provides this technology in a decentralized way? We identify a condition that depends only on benefit and cost terms which tells us when this technology is to be made available in the cities in a decentralized way. Finally, what are the properties of a policy regime that provides the technology in a centralized way with equal cost sharing by the cities? We obtain two conditions involving benefit and spatial spillover terms that describe scenarios in which (i) the technology is provided with majority voting in a city even though it is inefficient to do so and (ii) it is efficient to provide the technology in a city but majority voting will lead to this technology not being provided.



**Keywords:** Centralization, Decentralization, Political-Economy, Technology, Urban Crime

**JEL Codes:** K42, R11, R50

## 1. Setting the Scene

### *1.1. Preliminaries*

Urban crime is a salient issue in many of the world's large cities. In this regard, the work of Rainwater (2019) tells us that last year, "public safety" was one of the top ten concerns of city mayors all across the United States. Given the salience of urban crime, with one noteworthy lacuna in the literature that we describe in greater detail in sections 1.2 and 1.3 below, it is not surprising to find that this issue has given rise to a significant amount of primarily *empirical* and *case-study* based research from criminologists in particular and social scientists more generally. Consequently, there is at present a substantial literature that has analyzed the extent to which social disorganization, subculture, poverty, and conflict theories explain the reasons for the occurrence and the prevalence of urban crime.[5]

We learn from the research of Andreas and Price (2001) that the approaches adopted by cities to combat urban crime and the resources that these cities have made available to their police forces have changed dramatically with the passage of time.[6] For example, Carr (2017) informs us that police are now commonly using, *inter alia*, body cameras, in-vehicle computers, license plate readers, and gunshot detectors to fight crime.[7] Even though the use of body cameras by police has frequently been deemed acceptable---see Ariel *et al.* (2015)---the same cannot be said about the use of, for instance, facial recognition technologies. Gates (2002) and Schippers (2019) both note

---

5

See Ward (1976), Lynch (1981), Kohfeld and Sprague (1988), Hale (1996), White (1996), Gibbons (2004), Kourtit (2019), Lehmann (2019), and the many references cited in these sources for more on this and related issues.

6

Go to https://www.govtech.com/dc/articles/Police-Use-New-Technologies-to-Fight-Crime.html for additional details on this point. Accessed on 29 June 2020.

7

Go to https://www.thebalancecareers.com/technologies-that-are-changing-the-way-police-do-business-974549 for more on this point. Accessed on 29 June 2020.

that the use of facial recognition technologies to fight crime is controversial because there are significant legal, discrimination, and privacy related concerns about the use of such technologies. Conger *et al.* (2019) and Selinger and Hartzog (2019) contend that this explains, at least in part, why Berkeley, Oakland, and San Francisco (all in California), and Somerville (in Massachusetts), have now banned the use of facial recognition technologies by their police forces. Note that facial recognition technologies are controversial outside the United States as well. In this regard, the reporting of Boffey (2020) tells us that the European Union is now considering a temporary ban on the use of facial recognition technologies in public places.

Given the salience of new technologies such as facial recognition software in fighting urban crime, it is pertinent to ask what economists and regional scientists have written about the connections between fighting urban crime and the use of these new technologies to combat crime. Therefore, we now briefly discuss this literature and then proceed to the three main questions of our paper.

### *1.2. Literature review*

Cullen and Levitt (1999) empirically examine the link between rising city crime rates and urban flight in a variety of cities in the United States. Their analysis shows that almost all of the crime related decline in the population of cities is attributable to increased out-migration rather than to a decline in new arrivals. Does the use of information technologies affect the efficacy with which police fight crime? Garicano and Heaton (2006) explore the ways in which the use of information technologies influences the effectiveness of crime fighting from an empirical perspective. Their analysis of a panel data set of police departments covering the 1987-2003 time period demonstrates that the adoption of information technologies has substantial effects on a wide range of police organizational practices but a negligible impact on the effectiveness of crime fighting.

Palmer *et al.* (2012) study the use of computerized identity scanning technologies in Geelong, Australia. They contend that although these technologies have reduced alcohol related violence in the nightclub precinct of Geelong, discussions about the use of such technologies have tended to suppress concerns about information privacy and data security. The usefulness of "safe ride programs" is examined by Weber (2014) by using panel data for Milwaukee, Wisconsin. After comparing both the benefits and the costs of such programs, he concludes that "the safe ride program…is a relatively efficient means of reducing crime" (p. 1).

Is there a connection between vacant housing and urban crime? Price (2016) focuses on Jackson, Mississippi, and provides an answer to this question. He contends that consistent with the so called "Broken Windows" hypothesis, total crime is an increasing function of a neighborhood's level of degradation where degradation is measured by the level of vacant housing and the age of the housing stock. Examining the case of Memphis, Tennessee, Tulumello (2018) argues that policy reform at many levels is needed to address a situation in which social problems have become security issues.

Lacoe *et al.* (2018) provide a careful analysis of the nexuses between urban crime and private investment in the form of building permits in the "lagging neighborhoods" of Chicago and Los Angeles. These researchers show that although there is a clear relationship between crime and private investment, this relationship is not symmetric in the sense that private investment is sensitive to crime but only in rising crime contexts. This means that policies designed to reduce crime can serve the purpose of an economic development tool "but only in certain neighborhoods facing specific circumstances" (p. 154). Finally, Heywood and Weber (2019) examine the marginal contribution to urban safety in the city of Milwaukee, Wisconsin, provided by a university bus service when a so called "safe ride program" already exists in this city. The analysis undertaken by these researchers shows that the novel "eyes on the street" along the bus route along with increased transit use overall, that is, the sum of the safe rides and the new bus service rides, more than compensates for any potential effect of substitution away from the safe ride program.

Our review of the literature leads to two noteworthy conclusions. First, there are *no theoretical political-economy* studies that have analyzed whether controversial crime fighting technologies---such as facial recognition software---ought to be made available to city police forces. As noted by Friedman and Ferguson (2019) and Valentino-DeVries (2020), this is clearly an important public policy question in today's world and yet policy-makers such as mayors of cities, for instance, have no theoretical principles---that account for the economics and the politics of the underlying issue---upon which to base their decision-making about the provision of such contentious technologies. In this regard, what we would like to know is the following: Exactly how should policy-makers tradeoff the benefits and the costs associated with these controversial technologies?

Second, if it is determined, presumably on the basis of sound theoretical principles, that such contentious technologies are not to be made available to city police forces then, clearly, no further analysis is required. However, if it is decided that there exist circumstances in which such controversial technologies ought to be made available to city police forces then one salient question that arises next---and one on which there is *no* theoretical political-economy research---concerns the appropriate *governmental level* at which this provision decision ought to be made.

For example, should the governors of states in the United States be making this provision decision for cities in their state? If yes then this is an example of *centralized* decision-making. On the other hand, if the mayors of cities within a state make their own provision decisions then this is an example of *decentralized* decision-making. Given this dichotomy, what we would like to know is this: Which approach to decision-making leads to a more efficient allocation of a scarce crime fighting resource such as facial recognition software?

### *1.3. Objectives*

Given the absence of theoretical political-economy research on the two questions stated in the preceding two paragraphs, our central aim in this paper is to provide the *first* formal analysis of the properties of the decision to provide a controversial crime fighting technology to city police forces that takes economic and political factors into account explicitly.[8] Section 2 first provides a general discussion about why crime fighting technologies such as facial recognition software are controversial and then describes the theoretical political-economy framework in which there are three cities and that is adapted from Lockwood (2002). Section 3 first addresses the technology provision issue and then analyzes the properties of the decision to provide the technology in a *decentralized* fashion. Similarly, section 4 first deals with the technology provision issue and then examines the attributes of decision-making when the decision to provide a controversial crime fighting technology to the police force in the three

8

It is important to understand that because we are analyzing a theoretical model in this paper, it is *not* possible to account for *all* the factors that bear upon the decision to provide or not provide contentious crime fighting technologies *and* simultaneously ensure that the model is *tractable*. This explains why we have decided to focus on the economic and the political factors that are pertinent. However, this modeling strategy of ours should *not* be interpreted to mean that we believe factors other than economic and political ones are irrelevant in the decision to provide or not provide controversial crime fighting technologies. This last point is addressed in greater detail in section 2.1 below. Finally, our analysis is political-economic in nature because we use in our analysis, standard economic concepts such as benefits, costs, utility, and welfare and political concepts such as decentralized and centralized governmental decision-making and majority voting.

cities under consideration is made in a *centralized* manner with equal cost sharing by the three cities.[9] Section 5 first discusses our results and how they might be used in practice and then outlines four ways in which the research delineated in this paper might be extended.

## 2. Controversy and a Theoretical Framework

### *2.1. Why is facial recognition software contentious?*

We begin with a general discussion of five interrelated factors that together explain why crime fighting technologies such as facial recognition software are controversial in contemporary times. These factors pertain to (i) privacy, (ii) discrimination, (iii) misuse, (iv) errors, and (v) due process. Let us discuss each of these five factors in greater detail.

Facial recognition systems are built on computer programs that study images of human faces for the purpose of identifying them. Unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that does not require the knowledge, consent, or the participation of an individual. Therefore, a key concern is that this technology will be used for general, suspicion-less surveillance systems. State motor vehicles departments already possess high quality photographs of most citizens and these photographs are a natural source for facial recognition programs. The photographs themselves can easily be combined with public surveillance or other cameras to construct a thorough system of identification and tracking.[10]

9

Decentralized provision means that each city *independently* determines whether or not to provide a controversial crime fighting technology to its police force. In contrast, centralized provision means that a *central authority* in the aggregate economy determines whether or not a controversial crime fighting technology is provided to the police forces in each of the three cities under consideration.

10

Given this state of affairs, *privacy* advocates such as Magnet (2011), Silverman (2017), and Andrejevic and Volcic (2019) have pointed out that technologies such as facial recognition software lack proportionality in the sense that the benefits from the use of these technologies do not outweigh the costs stemming from the obvious intrusion into people's privacy. In addition, we are told that the systematic use of these technologies can lead to a situation in which public spaces, in general, are automated and subject to real-time surveillance.

Lohr (2018) notes that facial recognition technologies have improved dramatically with the passage of time and that some commercial software can now determine the gender of a person in a photograph. In particular, when the person in a photo is a white man, the software is right 99 percent of the time. However, the darker a person's skin color, the greater are the identification errors. In particular, when presented with the photographs of dark skinned women, the software can be wrong as much as 35 percent of the time. Therefore, from a policing standpoint, the available technology can be used to *discriminate* against people of color.

This point has been corroborated in a recent study by Bacchini and Lorusso (2019, p. 321). These authors point out that facial recognition technology, as used in western societies in contemporary times, buttresses existing racial disparities in stop, investigation, arrest, and incarceration rates because of what the authors call "racist prejudices." They then contend that this technology *discriminates* against disadvantaged racial groups such as black people because the technology "strengthens the unhealthy effects of racism…"[11]

---

Go to https://www.lexology.com/library/detail.aspx?g=e6cb3252-c9ec-4581-9857-2b58b2335c5c for additional details on these matters. Accessed on 30 June 2020.

11

See Feldstein (2019) for a discussion of related matters in an international setting.

As far as the *misuse* of facial recognition software is concerned, the key worry pointed out by Queally (2019) and Zizi (2019) is that facial recognition databases are *not* immune to hacking. This means that the available information could get into the wrong hands, and then could be used in malevolent ways. Other governments and hackers could gain access to an individual's picture, and any information stored along with it, including this individual's driver's license number, license plates, and more. Clearly, this kind of information can be dangerous when it is in the wrong hands. As such, cybersecurity measures will need to get stronger to protect all the available facial data, keep hackers at bay, and thereby preclude the *misuse* of the relevant data.

The use of facial recognition software in the context of policing is likely to have serious implications for individuals because this software is used to make stop, investigate, arrest, and incarcerate decisions. Therefore, Orcutt (2016), Crumpler (2020), and others have rightly pointed to the importance of minimizing *errors* by determining how accurate this software is. We learn that in ideal conditions, facial recognition software can have close to 100 percent accuracy. However, this degree of accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the individuals are clear and not obscured. In real world contexts, however, accuracy rates tend to be far lower.

Therefore, when using a specific facial recognition algorithm, it is important to consider the impact on accuracy and, the process, avoid the problem of *false positives*. Because facial recognition will likely be used in contexts where the user will want to minimize the likelihood of errors---such as when police mistakenly identify the wrong person when looking to identify suspects---algorithms are often set up to report a match only if they have a certain degree of confidence in their assessment. Using confidence thresholds of this sort is salient in situations where a human is not reviewing the matches made by an algorithm and where any *errors* can have serious impacts on those individuals who are misidentified.

Finally, we come to the *due process* factor. Generally speaking, due process is a legal requirement that the nation (United States) must respect all the legal rights that are owed to a citizen. In practice, due process seeks to balance the power of the government and protect citizens from the misuse of this power. So, when a government harms a citizen without following the exact course of the law, we have a due process violation.[12]

Specifically, the use of facial recognition software raises due process considerations because many observers believe that if this software is going to be used to secretly "identify" people and that these "identified" people can then be charged with a crime then the people involved have a right to obtain information about how the error-prone software actually functions and whether this software produced other matches in addition to the identified people. As pointed out by Gullo and Lynch (2019) and Valentino-DeVries (2020), the problem is that in some court cases, prosecutors have *not* disclosed information about how a particular facial recognition algorithm works and whether it produced other matches that were not considered by the prosecutor.

Facial recognition software is now being frequently used by police throughout the United States to identify suspects. Therefore, many observers find it inexplicable that the technology that can help to put a person in prison is used largely without either questions or oversight. When defendants confront lengthy prison sentences or even the death penalty, many believe---see Slaight and LeCloux (2020)---that stringent controls on the use of facial recognition software are essential.

---

12

Go to https://www.smokeball.com/blog/what-does-due-process-mean/ for a more expansive discussion of due process. Accessed on 1 July 2020.

In sum, defendants have a *due process* right to information about the algorithms used and the search results. We now proceed to discuss the modeling framework we utilize in the remainder of this paper.

### *2.2. The theoretical framework*

Consider an aggregate economy in which there are three cities denoted by $N = \{1, 2, 3\}$. The relevant authority---such as a mayor---in each city must decide whether to allow the police force in this city to have access to a controversial crime fighting technology. These three cities can be arranged in a linear manner or they can represent the three vertices of a triangle. In other words, the exact arrangement of these three cities in space is *not* important for our subsequent analysis in this paper. Actual examples of three cities that fit our theoretical framework include (i) Buffalo, Rochester, and Syracuse, in the state of New York, (ii) Chapel Hill, Durham, and Raleigh, in the state of North Carolina, and (iii) Cincinnati, Columbus, and Dayton, in the state of Ohio.

In the remainder of this paper, we shall think of the controversial technology as facial recognition software but the reader should note that the analysis we undertake is in *no way* dependent on this particular choice. In addition, we shall think of the decision to provide this crime fighting technology as being similar to the decision to provide a local public good. A local public good---see Hindriks and Myles (2013, chapter 7) for a textbook account---is a public good that is available only to the residents of a particular geographic area such as a city. In addition to the crime fighting technology that is of interest to us in this paper, other examples of local public goods include public parks and radio and television signals. That said, the reader should note that our model is more general than the recent analysis of Batabyal *et al.* (2019) because, unlike these researchers, we analyze the provision of a local public good in three and not two cities.[13]

We model the controversial aspect of facial recognition technology by supposing that in each city $i \in N$, this technology $t_i$ is either provided or not. In other words, the provision decision is *discrete* in nature. In symbols, this means that $t_i = \{0, 1\}$. In words, if $t_i = 0$ $(1)$ then the pertinent authority in city $i$ has decided to not provide (provide) the police force in this city with facial recognition technology.[14] If a decision is made in city $i$ to provide the police force with facial recognition technology $(t_i = 1)$ then it costs this city $c_i > 0$ units of a private good that is available to the residents of city $i$ for consumption purposes. The benefit to a resident of city $i$ from the provision of facial recognition technology is $b_i > 0$.

There is also a *spillover effect* from the provision of facial recognition technology $t_i$ in city $i$ to a resident of city $j \neq i$ which we denote by $s_{ij} \lesseqgtr 0$. This last inequality is meant to capture the idea that the spillover effect can in principle be either positive *or* negative. It would be positive, for instance, if city 1 decides not to provide facial recognition technology to its police force but city 2 does and a resident from city 1 visits city 2 and feels safer during his visit because the police force in city 2 is better able to deter crime by virtue of its use of facial recognition technology. The spillover would be negative if, for example, city 1 decides to make facial recognition technology

---

13

Two points are worth emphasizing now. First, we have already acknowledged that we are thinking of the provision of a crime fighting technology as being similar to the provision of a local public good. This means that our model is general in the sense that it can be used to analyze the provision of any good or service that has the attributes of a local public good. What this does *not* mean is that our model can be used to analyze the provision of "any urban service." Some urban services such as cable television and solid waste collection are very much like private goods and therefore they are commonly provided by private firms, sometimes under contract with a city or sometimes subject to some regulations. Second, in the context of crime fighting technologies such as facial recognition software, the provision decision is typically *discrete* and *not* continuous. In other words, this technology is either provided or it is not. As described in the next paragraph, we explicitly account for this point in our model and this is the specific connection between the provision of facial recognition software and our theoretical model.

14

We believe that the correct way to model the provision decision is as a discrete decision. That said, at the level of principle, it is possible to think of this decision as a continuous decision.

available to its police force and city 2 does not and, as a result, criminals move from city 1 to 2 and crime increases in city 2. Finally, the "own" spillover effect is clearly zero and we account for this by stipulating that $s_{ii} = 0$.

The three cities in our aggregate economy can be ranked in terms of the cost with which they are able to provide facial recognition technology to their respective police forces. In this regard, we suppose that $c_1 < c_2 < c_3$. This ranking means that city 1 is the *least cost* provider of facial recognition technology, city 2 occupies an intermediate position, and city 3 is the *highest cost* provider of facial recognition technology. Note that if $t_i = 0$ then clearly there is no benefit, cost, or spillover effect associated with this non-provision decision by city $i$.

Let us define the *set* of facial recognition technologies that are provided by $T = \{i \in N / t_i = 1\}$. The consumption of the private good by a resident of city $i$ is denoted by $x_i > 0$. We suppose that a resident of city $i$ is endowed with one unit of the private good and that this resident pays income tax denoted by $\tau_i > 0$. Clearly, this means that his consumption of the private good is given by $x_i = 1 - \tau_i$. Finally, the preferences of the residents in city $i$ are denoted by

$$u_i = \begin{cases} x_i + b_i + \sum_{\forall j \neq i} s_{ij} t_j, i \in T. \\ x_i + \sum_{\forall j \neq i} s_{ij} t_j, \ i \notin T. \end{cases} \tag{1}$$

The first (second) line on the right-hand-side (RHS) of equation (1) describes the utility obtained when facial recognition technology is (is not) provided by city $i$. Our next task is to use a political-economy perspective and analyze the properties of the decision by the relevant authority in city

$i$ to provide facial recognition technology to the police force in this city in a decentralized manner.

## 3. Decentralized Provision

### *3.1. Efficient provision of facial recognition technologies*

We begin by describing the *efficient* provision of facial recognition technologies in the three cities under study. At the same time, we also look at whether these technologies are provided or not. To this end, let us denote the total welfare from the provision of facial recognition technologies in cities 1, 2, and 3 by $W = \sum_{i=1}^{3} W_i$ where $W_i$ is the welfare in city $i$. Using equation (1), it is straightforward to confirm that the total welfare or $W$ is given by

$$W = \{1 - c_1 t_1 + b_1 t_1 + s_{12} t_2 + s_{13} t_3\} + \{1 - c_2 t_2 + b_2 t_2 + s_{21} t_1 + s_{23} t_3\} + \{1 - c_3 t_3 + b_3 t_3 + s_{31} t_1 + s_{32} t_2\}, \tag{2}$$

and it is understood that $t_i = \{0, 1\}$. The first, second, and third expressions in the curly brackets on the RHS of equation (2) denote the welfare in cities 1, 2, and 3, respectively.

To answer the question about whether facial recognition technology is or is not provided in each of the three cities under study, it will be helpful to rewrite the RHS of equation (2). This rewriting gives us

$$W = 1 + t_1\{b_1 - c_1 + s_{21} + s_{31}\} + 1 + t_2\{b_2 - c_2 + s_{12} + s_{32}\} +$$

$$1 + t_3\{b_3 - c_3 + s_{13} + s_{23}\}. \quad (3)$$

Inspecting equation (3), it is clear that in any city $i$, facial recognition technology will be provided by the responsible authority to the police force $(t_i > 0)$ as long as the condition $b_i - c_i + \sum_{\forall j \neq i} s_{ji} > 0$ holds. Otherwise, facial recognition technology will *not* be provided to the police force and, in symbols, this means that $t_i = 0$. The reader should understand that we have just answered the question "Should police in each of these three cities have access to such new and potentially controversial crime fighting technologies?" To see this clearly, note that even a controversial crime fighting technology such as facial recognition software has benefits and costs associated with it. In our model, for any city $i$, $b_i$ denotes the benefit, $c_i$ denotes the cost, and $\sum_{\forall j \neq i} s_{ji}$ denotes the sum of the spatial spillovers. So, if the *net benefit* from providing facial recognition technology or $b_i - c_i + \sum_{\forall j \neq i} s_{ji}$ is positive then this technology ought to be provided to the police in city $i$. If on the other hand, this net benefit is negative then the city ought not to provide this technology to its police force. Finally, in the knife-edge case where the net benefit is equal to zero, city $i$ is indifferent between providing and not providing this technology.

To conclude this discussion, note that we have now provided a clear answer to the question about when facial recognition technology ought to be provided to the police in the $ith$ city. So, if $b_i - c_i + \sum_{\forall j \neq i} s_{ji} < 0$ then the facial recognition technology is clearly *not* provided and that is the end of the story. That said, we contend that there are interesting special cases in which the spatial spillovers are handled differently and therefore these cases are worth analyzing in greater detail. As such, we now analyze the provision question when this provision is undertaken in a decentralized manner.

### *3.2. Role of spillover effects*

With decentralization, the decision to provide facial recognition technology to the police force in city $i$ is made in the city itself and, in this regard, we can write city $i's$ budget constraint as

$$\tau_i = c_i t_i. \tag{4}$$

Equation (4) tells us that in the $ith$ city, the expenditure on the facial recognition technology that is provided (the left-hand-side (LHS)) is equal to the receipt of revenue from the payment of income taxes by the city residents (the RHS).

The key point to recognize now is that the facial recognition technology will be provided to the police force in city $i$ as long as this provision raises city welfare *without* accounting for any spillover impacts. From equation (2), we know that the utility obtained in city $i$ when the facial recognition technology is provided to the police force in this city is given by

$$u_i = 1 - c_i t_i + b_i t_i + \sum_{\forall j \neq i} s_{ij}\, t_j. \tag{5}$$

So, ignoring the spillover effects means that we set the last term on the RHS of equation (5) or $\sum_{\forall j \neq i} s_{ij}\, t_j = 0$.

Using this last result in equation (5), we deduce that the facial recognition technology will be provided to the police force in city $i$ as long as the condition

$$b_i - c_i > 0 \tag{6}$$

holds. In words, with decentralized provision, facial recognition technology will be made available to the police force in any one of the three cities under consideration as long as the *city-specific* benefit to residents from such provision exceeds the *city-specific* cost to these same residents. Our final task in this third section is to first delineate the *set* of facial recognition technologies that is provided under decentralization and to then determine whether this decentralized provision of facial recognition technologies is efficient.

### *3.3. The provided set of technologies and efficiency*

Let us denote the *set* of facial recognition technologies that is made available to the police force in each city by $T^D$ and the *independent* provision decision in each city by $t_i^D$, where the superscript $D$ denotes decentralization. Now, some thought ought to convince the reader that, mathematically, the set we are interested in can be expressed as $T^D = \{i \in N / t_i^D = 1\}$.

Whether the above described decentralized provision of facial recognition technologies is or is not efficient will depend on the sign of the sum of spillovers term denoted by $\sum_{\forall j \neq i} s_{ji}$. As long as this sum of spillovers term is non-zero, that is, $\sum_{\forall j \neq i} s_{ji} \neq 0$, the decentralized provision of facial recognition technologies will ignore this term and therefore the resulting provision of facial recognition technologies will be *inefficient*. Put differently, the decentralized provision decision will be efficient only in the knife-edge case where the sum of spillovers term or $\sum_{\forall j \neq i} s_{ji} = 0$. We now proceed to analyze the attributes of decision-making in our aggregate economy when the decision to provide facial recognition technology to the police force in the three cities under consideration is made in a *centralized* manner.

## 4. Centralized Provision

### *4.1. Tax paid by city residents*

With centralization, the decision to provide facial recognition technologies in the three cities in our aggregate economy is made *not* in the individual cities but by a *central authority* with jurisdiction over all three cities. In addition, this central authority treats all three cities similarly and this means that there is *equal* cost sharing by all the cities under consideration. As noted in the first paragraph of section 2.2, one example of three actual cities that fit our model is Buffalo, Rochester, and Syracuse in the state of New York in the United States.

Denote the *set* of facial recognition technologies that are provided under centralization by $T^C$. Also, denote the facial recognition technology that is provided to the police force in city $i$ under centralization by $t_i^C$. Then, mathematically, the set of interest to us is given by $T^C = \{i \in N / t_i^C = 1\}$. We now want to derive an expression for the tax to be paid by any resident of city $i, i = 1,2,3,$ to fund the expenditure incurred in providing the facial recognition technology.

Using the logic of the budget constraint for city $i$ described in equation (4), we deduce that the tax payment to be made by any resident of city $i$ under centralization is given by $c_i t_i^C$. Also, since there is equal cost sharing by the three cities in our aggregate economy, a resident of the $ith$ city pays a tax given by

$$\tau_i = \frac{c_1 t_1^C + c_2 t_2^C + c_3 t_3^C}{3}. \qquad (7)$$

Inspecting equation (7), we see that the tax payable by any resident of city $i$ or $\tau_i$ is *increasing* in the three cost terms $(c_i^{\prime}s)$. In other words, the greater the cost---in terms of the private good---of providing facial recognition technology to the police forces in the three cities, the larger is the tax that the residents in any one city have to pay to fund this provision decision. We now determine the benefit to any resident of city $i$ from the set of facial recognition technologies that are provided under centralization.

### *4.2. Benefit received by city residents*

The benefit we seek is described by the utility function given in equation (1). Also, using the tax expression in equation (7), the consumption of the private good under centralization is $1 - \tau_i$. Therefore, putting these two pieces of information together, the complete expression for the benefit to any resident of city $i$ is

$$u_i = 1 - \frac{c_1 t_1^C + c_2 t_2^C + c_3 t_3^C}{3} + b_i t_i^C + \sum_{\forall j \neq i} s_{ij} t_j^C. \tag{8}$$

Observe from equation (8) that the facial recognition technology provided to the police force in city $i$ under centralization or $t_i^C$ affects the benefit to a resident of city $i$ in *opposite* ways. First, it directly *increases* utility through the $b_i t_i^C$ term on the RHS. Second, it *decreases* utility by virtue of its appearance in the $c_i t_i^C$ term in the numerator of the ratio expression on the RHS that describes in part the tax under centralization. We now analyze a noteworthy special case in which the spillover effects from the provision of facial recognition technologies in our aggregate economy are *uniform* and *positive*. In symbols, this means that $s_{ij} = s > 0, \forall i \neq j$.

*4.3. Uniform spillover effects*

To analyze this case in a meaningful manner, suppose that the facial recognition technology provision decisions are made by *majority voting*. This means that any city that would like to see its police force have access to this technology must secure the support of at least one other city. In this situation, what we would like to know is the following: What is the outcome of majority voting?

If the spillover effects are uniform and positive then the benefit expression given in equation (8) will need to be modified. This modification gives us

$$u_i = 1 - \frac{c_1 t_1 + c_2 t_2 + c_3 t_3}{3} + b_i t_i + \sum_{\forall j \neq i} s t_j. \tag{9}$$

Now, if the facial recognition technology is to be provided to the police force in city $i$ then, with majority voting, at least one other city must support this provision decision. This support will be forthcoming if and only if the sum of spillovers term *exceeds* the cost share. In other words, majority voting will result in city $i$ successfully providing its police force with facial recognition technology or $t_i > 0$ as long as the condition

$$s > \frac{c_i}{3} \tag{10}$$

holds.

Another way of expressing the outcome of majority voting is to say that this outcome is essentially ranked by the *cost*---in terms of the private good---of providing the facial recognition technology. Our final task in this paper is to compare the majority voting outcome with the efficient outcome.

***4.4. Majority voting and efficiency***

As in section 4.3, once again we suppose that the spillover effects from the provision of facial recognition technologies in our aggregate economy are uniform and positive. Now, from our analysis in section 3, it is straightforward to verify that in the *efficient* equilibrium, facial recognition technology will be provided to the police force in city $i$ as long as the following two inequalities

$$b_i - c_i + 2s > 0 \Rightarrow 2s > c_i - b_i. \tag{11}$$

hold.

In contrast, the inequality in (10) tells us that when there is centralized provision of facial recognition technology with majority voting, this technology will be made available to the police force in city $i$ only when

$$3s > c_i. \tag{12}$$

Comparing the inequalities in (11) and (12), it is clear that the efficient and the majority voting outcomes will be identical if and only if the uniform spillover term *equals* the benefit term or when $s = b_i$. Clearly, this is the knife-edge case and therefore we conclude that, in general, the centralized provision of facial recognition technologies will be *inefficient* whenever $s \neq b_i$. Two other points in this comparative exercise are worth emphasizing. First, if $s > b_i$ then there will be instances in which the facial recognition technology is provided with majority voting in city $i$ even though it is *inefficient* to do so. Second, if $s < b_i$ then we can have scenarios where it is *efficient* to provide facial recognition technology in city $i$ but majority voting will lead to this technology *not* being provided. This completes our political-economy analysis of decentralized versus centralized provision of urban crime fighting technologies in a model with three cities.

## 5. Conclusions

### *5.1. Discussion*

Given the contemporary concern---see Friedman and Ferguson (2019) and Valentino-DeVries (2020)---about whether our city police forces ought to have access to certain kinds of invasive anti-crime technologies, in this paper, we addressed the above concern by analyzing a theoretical model with three cities. Our analysis shed light on three broad questions.

First, we described the condition under which the police in each of the three cities under study ought to be provided with access to a controversial anti-crime technology such as facial recognition software. This condition involved looking at benefit, cost, and spatial spillover terms and then comparing the total benefit from the use of the anti-crime technology with the total cost. In order to use this condition in a practical setting, an appropriate authority will need to first determine the strength and the direction of the spatial spillovers. So, if the three cities under study are Buffalo, Rochester, and Syracuse in the state of New York, then since there is a lot of traffic between these three cities, these traffic flows will need to be monitored carefully. Second, residents of these three cities will need to be surveyed to obtain information on the benefits and the costs of using the anti-crime technology and criminal activity before and after the use of this technology will need to be recorded. Finally, the obtained information on benefits, costs, and spatial spillovers will need to be monetized---see Boardman *et al.* (2018) for additional details---to ascertain whether the *net benefit* from the use of an anti-crime technology is, in fact, positive.

Second, on the assumption that police are to have access to facial recognition technology, we discussed the properties of a policy regime in which this technology is made available in each of the three cities in a decentralized manner. So, continuing with the example of the three cities from the preceding paragraph, when the technology provision decision is decentralized, the mayors in Buffalo, Rochester, and Syracuse will make their *own* decisions about whether to make facial recognition software available in their cities *without* consulting with or taking any directives from the governor of the state of New York. The reader should note that although this decentralized approach protects the autonomy of cities in the sense that it allows cities to make a choice that is best for them, at the same time, this approach is problematic because it *disregards* the fact that Buffalo, for instance, may benefit or lose from the technology provision decision made by Rochester because of the presence of spatial spillovers.[15]

Finally and once again based on the supposition that police are to be provided with access to facial recognition technologies, we shed light on the characteristics of a policy regime in which the technologies are made available in a centralized manner with equal cost sharing by the three cities. The main policy implication from our analysis here is that except in one specific case, the centralized provision of facial recognition technology in the presence of majority voting will be *inefficient*. Practically, this means that majority voting is *not* necessarily the best way to decide

[15] The only instance in which this last point does not apply is when the spatial spillovers sum to zero.

whether facial recognition technology should be made available to the police force in a particular city.[16]

### *5.2. Extensions*

We now conclude with four examples of the ways in which the research delineated in this paper might be extended. First, it would be useful to analyze a dynamic version of our model in which the pertinent city authority can *learn* about how useful facial recognition technology actually is in reducing urban crime and then use this learning to potentially alter its decision-making in subsequent time periods. Second, it would also be helpful to collect data and determine the strength and the direction of the spillover effects that we have discussed in our analysis. Third, one could construct an expanded model that includes privately owned anti-crime technologies (security cameras on private property) and then shed light on the usefulness of public-private initiatives that share personal or private data. Finally, given the existence of spatial spillovers, one could use the work of Greenberg *et al.* (2002) and Oladi (2005) to see how useful it would be to analyze the provision of facial recognition technology as a game between different cities. Studies that analyze these aspects of the underlying problem about the effectiveness of facial recognition technologies will provide additional insights into the nexuses between contentious crime fighting technologies on the one hand and actual urban crime reduction on the other.

16 See Snoddon (1994) for additional details on this and related matters.

## References

Andreas, P., and Price, R. 2001. From war fighting to crime fighting: Transforming the American national security, *International Studies Review*, 3, 31-52.

Andrejevic, M., and Volcic, Z. 2019. "Smart" cameras and the operational enclosure. Forthcoming, *Television and New Media*.

Ariel, B., Farrar, W.A., and Sutherland, A. 2015. The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial, *Journal of Quantitative Criminology*, 31, 509-535.

Bacchini, F., and Lorusso, L. 2019. Race, again: How face recognition technology reinforces racial discrimination, *Journal of Information, Communication, and Ethics in Society*, 17, 321-335.

Batabyal, A.A., Kourtit, K., and Nijkamp, P. 2019. Using local public goods to attract and retain the creative class: A tale of two cities, *Regional Science Policy and Practice*, 11, 571-581.

Boardman, A.E., Greenberg, D.H., Vining, A.R., and Weimer, D.L. 2018. *Cost-Benefit Analysis*, 5th edition. Cambridge University Press, Cambridge, UK.

Boffey, D, 2020. EU eyes temporary ban on facial recognition in public places, *The Guardian*, 17 January, https://www.theguardian.com/technology/2020/jan/17/eu-eyes-temporary-ban-on-facial-recognition-in-public-places. Accessed on 1 July 2020.

Carr, J.B. 2017. Estimating the effects of police technology using quasi-experimental methods, *Journal of Benefit-Cost Analysis*, 8, 360-368.

Conger, K., Fausset, R., and Kovaleski, S.F. 2019. San Francisco bans facial recognition technology, *New York Times*, 14 May, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Accessed on 1 July 2020.

Crumpler, W. 2020. How accurate are facial recognition systems---and why does it matter? *Center for Strategic and International Studies*, 14 April, https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. Accessed on 1 July 2020.

Cullen, J.B., and Levitt, S.D. 1999. Crime, urban flight, and the consequences for cities, *Review of Economics and Statistics*, 81, 159-169.

Feldstein, S. 2019. How artificial intelligence is reshaping repression, *Journal of Democracy*, 30, 40-52.

Friedman, B., and Ferguson, A.G. 2019. Here's a way forward on facial recognition, *New York Times*, 31 October, https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html. Accessed on 1 July 2020.

Gates, K.A. 2002. Wanted dead or digitized: Facial recognition technology and privacy, *Television and New Media*, 3, 235-238.

Garicano, L., and Heaton, P. 2006. Computing crime: Information technology, police effectiveness, and the organization of policing, Center for Economic Policy Research *Discussion Paper 5837*.

Gibbons, S. 2004. The costs of urban property crime, *Economic Journal*, 114, F441-F463.

Greenberg, J., Luo, X., Oladi, R., and Shitovitz, B. 2002. (Sophisticated) stable sets in exchange economies, *Games and Economic Behavior*, 39, 54-70.

Gullo, K., and Lynch, J. 2019. When facial recognition is used to identify defendants, they have a right to obtain information about the algorithm used on them, EFF tells court, *Electronic Frontier Foundation*, 12 March, https://www.eff.org/ru/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain. Accessed on 1 July 2020.

Hale, C. 1996. Fear of crime: A review of the literature, *International Review of Victimology*, 4, 79-150.

Heywood, J.S., and Weber, B. 2019. University-provided transit and crime in an urban neighborhood, *Annals of Regional Science*, 62, 467-495.

Hindriks, J., and Myles, G.D. 2013. *Intermediate Public Economics*, 2nd edition. MIT Press, Cambridge, MA.

Kohfeld, C.W., and Sprague, J. 1988. Urban unemployment drives urban crime, *Urban Affairs Review*, 24, 215-241.

Kourtit, K. 2019. *The New Urban World*. Shaker, Aachen, Germany.

Lacoe, J., Bostic, R.W., and Acolin, A. 2018. Crime and private investment in urban neighborhoods, *Journal of Urban Economics*, 108, 154-169.

Lehmann, S. 2019. *Urban Regeneration*. Palgrave Macmillan, London, UK.

Lockwood, B. 2002. Distributive politics and the costs of centralization, *Review of Economic Studies*, 69, 313-337.

Lohr, S. 2018. Facial recognition is accurate, if you're a white guy, New York Times, 9 February, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html. Accessed on 1 July 2020.

Lynch, K.A. 1981. *A Theory of Good City Form*. MIT Press, Cambridge, MA.

Magnet, S.A. 2011. *When Biometrics Fail*. Duke University Press, Durham, NC.

Oladi, R. 2005. Stable tariffs and retaliations, *Review of International Economics*, 13, 205-215.

Orcutt, M. 2016. Are face recognition systems accurate? Depends on your race, MIT Technology Review, 6 July, https://www.technologyreview.com/2016/07/06/158971/are-face-recognition-systems-accurate-depends-on-your-race/. Accessed on 1 July 2020.

Palmer, D., Warren, I., and Miller, P. 2012. ID scanning, the media, and the politics of surveillance in an Australian regional city, *Surveillance and Society*, 9, 293-309.

Price, G.N. 2016. Broken windows and crime in development challenged urban areas: Evidence from Jackson, Mississippi USA, *Journal of Developing Areas*, 50, 209-220.

Queally, J. 2019. Facial recognition data collected by U.S. customs agency stolen by hackers, Salon, 11 June, https://www.salon.com/2019/06/11/facial-recognition-data-collected-by-u-s-customs-agency-stolen-by-hackers/. Accessed on 1 July 2020.

Rainwater, B. 2019. The 10 biggest issues U.S. mayors say they're tackling in 2019, https://www.fastcompany.com/90363344/the-10-biggest-issues-u-s-mayors-say-theyre-tackling-in-2019. Accessed on 1 July 2020.

Schippers, B. 2019. Facial recognition: Ten reasons you should be worried about the technology, *The Conversation*, 21 August, https://theconversation.com/facial-recognition-ten-reasons-you-should-be-worried-about-the-technology-122137, Accessed on 2 July 2020.

Selinger, E., and Hartzog, W. 2019. What happens when employers can read your facial expressions? *New York Times*, 17 October, https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html. Accessed on 1 July 2020.

Silverman, J. 2017. Privacy under surveillance capitalism, *Social Research*, 84, 147-164.

Slaight, J., and LeCloux, R. 2020. Facial recognition technology: Balancing safety and privacy, *Wisconsin Policy Project*, 3, 1-17, https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/facial_recognition_privacy_3_4.pdf. Accessed on 1 July 2020.

Snoddon, T.R. 1994. Majority voting and local public goods: Does myopia matter? *Canadian Journal of Regional Science*, 17, 169-187.

Tulumello, S. 2018. The multisector nature of urban security and public safety: Crime prevention from local policy to policing in Lisbon (Portugal) and Memphis (the United States), *Urban Affairs Review*, 54, 1134-1169.

Valentino-DeVries, J. 2020. How the police use facial recognition, and where it falls short, *New York Times*, 12 January, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html. Accessed on 1 July 2020.

Ward, B. 1976. *The Home of Man*. W.W. Norton and Company, New York, NY.

Weber, B. 2014. Can safe ride programs reduce urban crime? *Regional Science and Urban Economics*, 48, 1-11.

White, J.D. 1996. The map of the city: Putting an Asian face on crime, *Technological Forecasting and Social Change*, 52, 199-219.

Zizi, M. 2019. The flaws and dangers of facial recognition, *Security Today*, 1 March, https://securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx. Accessed on 1 July 2020.