Digital Vulnerability: The Unequal Risk of E-Contact with the Criminal Justice System

ROBERT VARGAS, KAYLA PREITO-HODGE, AND JEREMY CHRISTOFFERSON

Increased citizen interaction with the criminal justice system on digital platforms renders citizens more vulnerable to breaches of information to third parties. We introduce the concept of digital vulnerability to measure the extent to which technology produces unequal exposure to risk of data breaches. Using police-dispatcher radio communication, we examine the extent to which dispatchers reveal identifiable information about callers reporting crime. Data come from sixty audio-recorded hours of police-dispatcher radio communication across three racially distinct police radio zones in Chicago. Findings revealed that one of every ten calls made to police in zones serving racial minorities disclosed caller names or home addresses. We discuss implications for research on racial inequality in criminal justice contact, police-community relations, and policies concerning police-dispatcher radio communication.

Keywords: criminal justice contact, 911 emergency service, policing, technology, race

Of the 240 million calls made to 911 every year, a significant portion are for police assistance (NENA 2017). In Chicago alone, from 2000 to 2010, 911 dispatchers made an annual average of five million calls for police service on citizens' behalf. This form of electronic contact, or e-contact, with the criminal justice system occurs more frequently than physical forms of criminal justice contact, such as the twelve million individuals arrested or the eleven million individuals jailed each year in the United States (Federal Bureau of Investigation 2013). Equally important is that details about these calls for assistance can be heard by anyone over public radio frequencies. Most city police departments and 911 dispatchers still rely on open access radio frequencies to communicate, meaning that anyone with a radio, cell phone,

Robert Vargas is Neubauer Family Assistant Professor of Sociology and director of the Violence, Law, and Politics Lab at the University of Chicago. **Kayla Preito-Hodge** is a graduate student in the sociology department at the University of Massachusetts-Amherst and a recipient of the National Science Foundation's Graduate Research Fellowship. **Jeremy Christofferson** is a graduate student in the sociology department at the University of Notre Dame.

 Vargas, Robert, Kayla Preito-Hodge, and Jeremy Christofferson. 2019. "Digital Vulnerability: The Unequal Risk of E-Contact with the Criminal Justice System." *RSF: The Russell Sage Foundation Journal of the Social Sciences* 5(1): 71–88. DOI: 10.7758/RSF.2019.5.1.04. We thank Ariel Azar and Anil Sindhwani for research assistance on this project, as well as Dan Gillion, Jothie Rajah, the American Bar Foundation, the Russell Sage Foundation, and the anonymous reviewers for comments and critiques on earlier components of this article. Direct correspondence to: Robert Vargas at robvargas@uchicago.edu, 1126 E. 59th St., Chicago, IL 60637.

or computer can eavesdrop on police-dispatcher communication.[1] On the one hand, this enables journalists or citizen groups to monitor and scrutinize police behavior; on the other, it provides criminals, gangs, or predatory businesses with the ability to collect personal information about citizens for malicious or exploitive purposes (Jacobs 2015; Lageson 2016; Vargas 2016).

The ease by which police-dispatcher communication can be compromised is one of many recent examples of how technological advances in the administration of criminal justice policies is having detrimental and often unintended consequences for citizens. The challenge of protecting callers' or witnesses' identities is becoming even more challenging as police departments incorporate "big data" in their everyday activities (Jacobs and Wright 2006; Brayne 2017). Similarly, the advent of criminal record databases is placing citizens at greater risk of having their personal information hacked or exploited by third parties (Jacobs 2015; Lageson 2016; Vuolo, Lageson, and Uggen 2017). The adoption of new technologies is increasing citizens' e-contact with the criminal justice system and, in doing so, producing new forms of digital racial inequalities.

This article introduces the concept of *digital vulnerability* to help scholars begin to unpack the extent to which e-contact with the criminal justice system is placing citizens at unequal risk of harm. Digital vulnerability refers to citizens' risk of having incriminating information publicly disclosed and exploited by third parties. Although the article focuses on 911 calls, digital vulnerability is a concept that can be applied more broadly to other criminal justice technologies.

We introduce digital vulnerability through a comparative case study of interaction between police officers and 911 dispatchers over public radio frequencies in Chicago. Using sixty hours of audio recordings across three radio zones, defined as bounded geographical areas in which officers and dispatchers communicate, we examine the extent to which officers or dispatchers disclose identifiable information about callers: the caller's first name, last name, or home address. Each radio zone in the study served a demographically distinct community—the first predominantly African American, the second predominantly white, and the third predominantly Latino.

Findings revealed startling racial inequality in digital vulnerability. Black and Latino communities had far greater digital vulnerability than white communities. Approximately one of every ten calls made to police in zones serving racial minorities disclosed identifiable information about the caller—12 percent for blacks (44 of 371 calls), 8 percent for Latinos (11 of 148). In contrast, not a single call of 121 in the white police zone disclosed identifiable information. When we exclude citizen calls for direct police assistance, where the caller is in immediate danger and needs help at their home address, the inequality is even greater. Forty percent of third-party calls (47 of 116) in the black radio zone and 25 percent in the Latino (30 of 120) revealed identifiable information, whereas none of the forty-three in the white radio zone revealed identifiable information. In Chicago, where gangs have been shown to retaliate against residents who call police as well as use police radio scanners to identify callers in order to retaliate, these data disclosures put racial minorities at greater risk of harm than whites (Hagedorn 2015; Venkatesh 2006; on scanners, Vargas 2016).

Our findings have several implications. First, we show that digital vulnerability can be a useful concept for identifying inequalities rooted in technology and citizen e-contact with the criminal justice system. For example, our study reveals that the lack of citizen cooperation with police may stem not only from instances of overt police brutality or cultural dispositions, but also from local government's inability to digitally protect callers' identities (Desmond, Papachristos, and Kirk 2016; Kirk and Papachristos 2011). Second, our findings

1. One of the arguments police use for continuing use of open radio frequencies is the ease of communication it allows across city agencies in the event of a major emergency. Encrypting a communication channel (whether radio or digital) would require agencies to bypass security interfaces, which may delay or inhibit interagency coordination.

show the importance of studying intermediaries such as 911 dispatchers, who are trusted to provide private information about citizens to agents of the criminal justice system. Such intermediaries, though well intentioned, may unknowingly be doing more harm than good to citizens. Finally, as one of the first to systematically examine police-dispatcher communication, this study has policy implications for training emergency dispatchers as well as for debates over regulating public access to police radio frequencies.

TECHNOLOGY AND CRIMINAL JUSTICE CONTACT

Technological advances in media and communication are pivotal symbols of economic progress in society, but these advances have also accelerated growth in surveillance practices, hacking, and data breaches. With respect to law enforcement, technological advances are making citizen e-contact with the criminal justice system more prevalent. For example, local governments are increasingly using big data to learn more about wanted or "potential" criminals through algorithms estimating citizens' likelihood of committing crime (Asher and Arthur 2017). Police are also collecting data on citizens by sifting through databases produced by other governmental agencies such as immigration, social security, and departments of children and family services (Brayne 2017; Stuart 2016). Scholars describe such integration as parallel state structures, whose left and right hands govern disadvantaged populations through welfare and criminal justice policy (Soss, Fording, and Schram 2011).

Despite the growth of citizen e-contact with the criminal justice system, much of the literature to date has focused on physical contact between law enforcement agents and citizens through arrests or police stops. Researchers have used cross-sectional or longitudinal data on individuals to show how experiencing incarceration, arrest, or conviction can negatively affect health (Massoglia and Pridemore 2015; Turney 2014), political participation (Manza and Uggen 2008; Sugie 2015), and economic life chances (Wakefield and Wildeman 2013). Contact with the criminal justice system is thought to affect individuals physically, organizationally, or legally. For example, experiencing arrest or incarceration can be a stressor that, compounded with others, has deleterious effects on mental or physical health (Sewell and Jefferson 2016; Sugie and Turney 2017). Similarly, the trauma of incarceration or police brutality can operate organizationally, formerly incarcerated individuals being less likely to participate, apply for, or seek help from public agencies (Brayne 2014; Desmond, Papachristos, and Kirk 2016). Contact also has legal effects, in that laws that disenfranchise ex-convicts from employment or social services create poverty traps for the formerly incarcerated (Pager 2003).

Digital or electronic forms of contact have been less explored, but a handful of scholars are charting important new ground in this area by studying online criminal record databases (Lageson 2016; Jacobs 2015; Vuolo, Lageson, and Uggen 2017). Companies that run these databases acquire criminal information from the federal government for mass distribution on the internet (Jacobs 2015). These websites include mug shots and police reports of the accused and have the reputation of presenting false and misleading information. Sarah Lageson argues that such sites constitute a new form of punishment and discrimination for individuals impacted by the criminal justice system, many of whom are unaware these records even exist (2016).

By typing the names of job applicants into a search engine, employers are provided a baseless platform on which they can judge applicants' moral character. Proponents of online criminal record databases argue that their services fulfill the "public's right to know." Scholars, however, maintain that these databases are far from genuine in intent and are financially exploitative and socially damaging (Jacobs 2015; Lageson 2016; Vuolo, Lageson, and Uggen 2017). For instance, on Mugshots.com, web publishers disclaim the accuracy of the records on the database, but refuse to remove the information in the event an individual is found not guilty or the case is dismissed—ultimately leaving permanent marks of criminality. Third-party companies, such as Internetreputation.com, advertise their removal services for hun-

dreds of dollars a month to individuals damaged by online criminal record databases. James Jacobs argues that these companies are highly predatory and that "On the surface, the mug shot sites and the reputation firms are mortal enemies. But behind the scenes, they have a symbiotic relationship that wrings cash out of the people exposed" (2015, 84). Laws governing the dissemination of private criminal information online remain largely absent; however, some states have begun taking preventative approaches by regulating how criminal justice agencies disseminate citizens' personal information (Jacobs 2015).

Law enforcement and private companies are not the only actors seeking private electronic information about citizens. Criminal groups do as well. In the age of the internet, hackers have targeted government databases to steal citizen identities. For example, in 2015, a group of hackers broke into databases of the Office of Personnel Management and stole 20.5 million social security numbers (Davis 2015). Similar data breaches have occurred among local governments in Minnesota, Georgia, and California. Hackers have even compromised some of the most secretive government agencies, such as the National Security Administration and Internal Revenue Service (Shane, Perloth, and Sanger 2017).

Stealing sensitive information about citizens from government data sources does not require significant technological expertise. With respect to policing, technological advances have made it easy for anyone with a smart phone, tablet, or computer, to listen and monitor police radio communication at any time and from any location on the planet. Prior to the internet, listening to police chatter over radio frequencies required purchasing a handheld scanner and doing research to learn the frequencies and geographies in which police communicated. Journalists were the most likely to be adept at these skills, given their goal to be the first to break a news story.

Today, monitoring police scanners is becoming more common among criminal groups. Some use scanners while committing a crime to learn precisely when police are on their way to the scene (Liebowitz 2012). Most troubling are criminal groups that monitor police radio communication to conduct countersurveillance on citizens reporting crimes to police (Vargas 2016). Scholars of organized crime have long argued that Omerta, or code of silence, is essential to the survival of organized criminal groups (Gambetta 1996; Sanchez-Jankowski 1991). Omerta is an informal expectation that criminal groups enforce through the threat of violence that no citizen is to report the organization's activities to police or cooperate with any police investigations (Gambetta 1996). In the United States, Omerta is often referred to as an inner-city code of silence, which scholars have found among Mexican and African American organized criminal groups (Vargas 2016; Venkatesh 2006).

The practices and policies of police-dispatch communication provide another way to explore inequalities generated through e-contact with the criminal justice system. While providing police with as much information as possible can expedite calls for service, dispatchers may be unaware of the consequences resulting from divulging identifiable information about callers over public radio frequencies.

DIGITAL VULNERABILITY

The notion of vulnerability is familiar in the criminal justice contact literature and sociology more broadly. It is the idea that social structures render groups more likely to experience pain, suffering, or marginalization than others (Fineman 2008). The idea of a digital vulnerability extends prior research by emphasizing that citizen vulnerability occurs not only physically during police stops on the streets or trials in county courts, but also digitally across cyberspace and radio waves. It concerns governments' ability to safeguard citizen's private information from groups with malicious intentions. Therefore, we define digital vulnerability as citizens' risk of having incriminating information publicly disclosed and exploited by third parties. By defining digital vulnerability this way, we aim to advance research identifying inequalities generated by the criminal justice system's use of technology.

We use radio communication between 911 dispatchers and police officers to assess the degree of digital vulnerability across three racially distinct geographical areas in Chicago. The

goal is to assess how much identifiable information is revealed about callers that criminal groups could use to retaliate which, in turn, would have deleterious consequences on police-community relations. The concept of digital vulnerability, however, is not meant to be unique to citizens' 911 phone calls. Other forms of e-contact with the criminal justice system may render citizens digitally vulnerable to a wider variety of consequences than retaliation from criminal groups. For example, in Chicago, police collect data on Latino youth in disadvantaged neighborhoods and erroneously label many as "gang affiliated" (Serrato 2017). Other government agencies looking to employ or provide services to Latino youth can access these data when running background checks, which can lead to unwarranted denials of jobs or benefits. Thus, living in a disadvantaged neighborhood with high degrees of e-contact with the criminal justice system can render certain populations more digitally vulnerable to a host of negative consequences.

THE RISKS OF DIGITAL VULNERABILITY OVER POLICE RADIO FREQUENCIES IN CHICAGO

This study of digital vulnerability over police radio frequencies was motivated by a systematic qualitative study on citizen police reporting in Chicago, conducted by the lead author, that discovered the risks of dispatchers disclosing identifiable information about callers. After canvassing sixty randomly selected blocks of Chicago's Little Village neighborhood, Robert Vargas identified a cluster of eight blocks where the majority of residents refused to report crimes to police because allegedly corrupt officers disclosed caller identities directly to gang members (2016). To assess the validity of residents' allegations against police, Vargas conducted additional fieldwork with gang members and police officers on residential blocks and discovered that gang members were identifying callers by monitoring police radio communication, retaliating by firebombing callers' houses, and spreading misinformation by claiming the police had intentionally "ratted out" residents.

"You got to understand," said Freddy, a former gang member, "some of the gang members have police scanners. Not just any scanner, but the actual police scanner. So when cops make the call, they hear caller's names and addresses."

Vargas confirmed these findings by directly observing gang members with police scanners in their possession and learning addresses of residents with whom the gang had retaliated. Gang members acquired police-issued scanners by breaking into police squad cars, and regularly used them to, as one gang leader described, "listen in on what the cops were up to" as well as "tell [residents] it was the cops who ratted them out to scare the shit out of them" (2016, 131).

Through interviews with gang members, Vargas learned the addresses of seven residents against whom the gang had retaliated as a result of information disclosed over police radio frequencies. In each of the retaliated households, residents had called 911 to report witnessing gang members carrying weapons or acting suspiciously, only to have their homes set on fire within the next twenty-four hours. In the aftermath of these fire bombings, gang members engaged in additional work of deceiving residents by claiming that corrupt police officers intentionally disclosed caller identities to the gang. In total, Vargas identified seven instances of gang members identifying and retaliating against residents through monitoring police radio communication between 2009 and 2011, which influenced residents on these four blocks to refrain from reporting crime to police (2016). Aside from the Chicago context, researchers have similarly found gangs or criminals listening to police radio communication to either retaliate against residents or evade police capture in Maryland (Liebowitz 2012), Washington, D.C. (Paquette 2015), and St. Louis (Patrick 2014).

Ideally, one would survey gangs of Chicago to assess the extent to which they monitor police radio communication and retaliate against callers, but such an approach is not feasible given the low likelihood that these groups would readily divulge such information. Thus, in this study, we aim to advance this line of inquiry by examining the extent to which residents are vulnerable to retaliation by having identifiable information disclosed over open

Table 1. Radio Zone Characteristics

	White Zone 4	Black Zone 8	Latino Zone 13
Frequency	460.15	460.2	460.45
Police districts	1, 18	4, 6	9
Neighborhoods	Gold Coast, Lincoln Park	Auburn-Gresham, Chatham	Bridgeport, Brighton Park, New City
Total population	156,424	77,201	156,424
Number of gangs	2	7	15
Homicide rate	2	40	28
Citizen complaints	1.04	4.77	0.87

Source: Authors' calculations based on American Community Survey five-year Estimates, 2010–2015 (U.S. Census Bureau 2016); Invisible Institute 2016; City of Chicago Data Portal 2016; Chicago Crime Commission 2012.
Note: Rates are per 100,000.

airwaves. To do so, we systematically examined police radio communication across three geographical areas of Chicago.

METHODS AND COMPARATIVE CASE STUDY DESIGN

The Chicago Police Department is structured into twenty-five geographical administrative units known locally as districts. In these districts, 911 dispatchers relay calls for service to patrol officers across fourteen radio zones, each having a unique frequency. Data for this study come from sixty hours of audio recordings across three police radio zones, twenty hours per zone. In each zone, we recorded one-hour increments from 7 to 8 p.m. and from midnight to 1 a.m., Monday through Friday, for two weeks. Audio recordings were conducted in July of 2016 for zones 8 and 13, and July through August of 2017 for zone 4. We recorded audio from police radio zones using www.broadcastify.com, a free website that plays a live feed of all police radio zones on the internet. We played the radio zones on loud speakers and used a handheld recording device to record audio.[2]

To assess racial differences, we sampled three police radio zones that served racially homogenous neighborhoods. Zone 8 included patrol officers from districts 4 and 6, which served the predominantly black neighborhoods of Auburn-Gresham and Chatham. Zone 13 included district 9, which served the predominantly Latino neighborhoods of Brighton Park, Bridgeport, and New City. Zone 4 included districts 1 and 18, which served the predominantly white and affluent downtown central business district, the Gold Coast, and Lincoln Park.

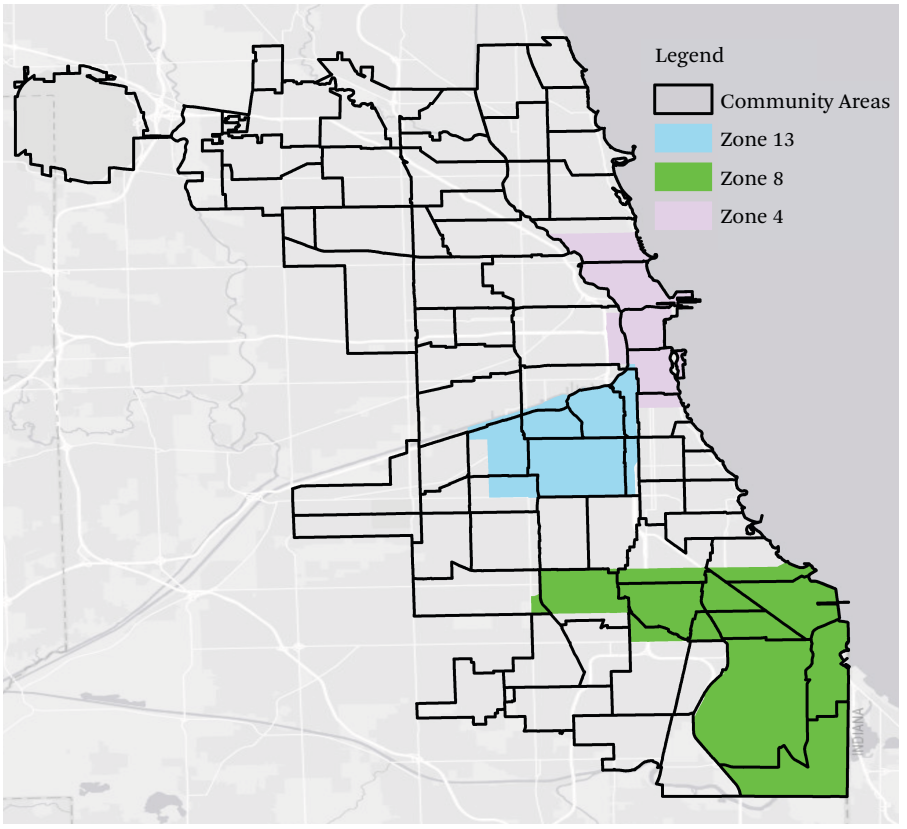
Table 1 provides an overview of each radio zone's characteristics derived from census data averaged across the police districts or neighborhoods in each zone. The figures in table 1 should be interpreted with some caution as the neighborhood and police radio zone boundaries do not perfectly match (see figure 1).

The black and Latino radio zones had high homicide rates, rates of citizen complaints against police officers, and greater presence of street gangs.[3] Zone 8 serves neighborhoods home to infamous black gangs like the Black P. Stones, Gangster Disciples, and the Black Disciples. Zone 13 is home to violent Latino gangs such as the Maniac Latin Disciples, Satan Disciples, and Insane Spanish Cobras. Disclosing identifiable information about callers in

2. For this study, we do not have access to interactions between callers and 911 dispatchers. Audio of citizen calls to 911 dispatchers in Illinois are only accessible to researchers making Freedom of Information Act (FOIA) requests within thirty days that the call was made. This severely hampers any effort to systematically assess audio of 911 calls over time.

3. Data on citizen complaints against officers from the Invisible Institute's citizen police data project, which aggregates the number of complaints filed against police officers at the district level. Our calculation is based on the sum of complaints across districts in each zone from 2010 to 2015.

Figure 1. Locations of Police Zones in Chicago Community Areas



Source: City of Chicago Radio Communications 2016.

these gang-infested areas heightens the risk of citizens' digital vulnerability in these radio zones.

To analyze the data, we conducted multiple rounds of coding using the audio coding tool in NVivo. We spliced the calls in the audio files into segments and assigned each a unique ID. These audio segments were instances of dispatchers introducing calls for service to a police officer. Segments ranged between ten and forty-five seconds depending on how much information the dispatcher provided. Consider the following example of how we coded a segment, using pseudonyms, when a dispatcher introduced a new call for service to a police officer:

> Call 71
> DISPATCHER: 723, check for a suspicious person at 73rd and Vincent. A woman named Jennifer says there are two vehicles following her. She lost sight of them, but is scared to go home. One was a tan Toyota Camry, the other was a gray Astro van.

Sometimes chatter between officers and dispatchers for a case such as call 71 would continue for a few minutes while other calls would come in, thereby increasing the difficulty in following the thread of a conversation over time. Thus, to have as clean a sample as possible, we only coded the first interaction between the dispatcher and officer, such as in call 71, to avoid miscoding prolonged radio chatter to wrong calls. A total of 650 calls like call 71 formed the sample of our study.

The next round of coding consisted of entering call characteristics into an Excel spreadsheet. Specifically, we coded as zero (no) or 1 (yes) the following characteristics of each call: address provided for crime scene, first name

of caller disclosed, last name of caller disclosed, home address of caller disclosed, and whether the caller was described as anonymous. In addition, we coded the type of crime for each call, as well as the date, time, and district where it occurred.

Most important, we coded for whether the caller was requesting direct assistance from police or requesting police assistance as a third-party or bystander. This distinction is crucial for our analysis because callers requesting direct assistance, like the woman in call 71, need to give identifiable information to receive help as soon as possible. As our study focuses on digital vulnerability, third-party calls are of most relevance to our analysis. Consider the following example of a third-party call:

> Case 86
> DISPATCHER: Suspicious person. 6000 S. Main Street. John Smith is calling. Male black, bald, and a mustache. White shirt, black shorts. Walking northbound trying to hold up people for money. John's family members trying to get more information by going door-to-door.

From the audio, we can deduce that a man named John Smith called police to investigate a suspicious person attempting to rob people on the street. In this example, we code the call with a 1 indicating that the call reported the address of the crime scene. Although the dispatcher did not disclose the caller's home address, he did disclose the caller's first and last name and shared that the caller's family was seeking more information from neighbors, which suggests that the caller lived on that block or nearby. Such a call, we argue, exemplifies dispatchers rendering citizens digitally vulnerable to retaliation from gangs. Third-party calls, rather than calls for direct assistance from people needing immediate police assistance, are the focus of our analysis across police radio zones.

To protect the privacy of callers, police officers, and dispatchers in this study, we used pseudonyms throughout the analysis and presentation of results. The audio files contain identifiable information, and we stored these data in a password-protected computer with no internet access. According to Illinois law and the Federal Communications Commission (FCC), police radio communication is considered public record, and can thus be recorded, analyzed, and scrutinized (FCC 2008). However, in the spirit of protecting the privacy of callers, police officers, and dispatchers, we use pseudonyms for all individuals in this study.

The process of coding and cleaning the data took six months. Afterward, we created graphs describing findings across the three police zones. In addition, we use two measures to calculate digital vulnerability across each radio zone. The first measure is the share of total calls with disclosed identifiable information, which uses the sum of direct-assistance calls and third-party calls as the denominator. The second measure is the share of third-party calls with disclosed identifiable information, which only uses third-party calls as the denominator. Last, we report our findings as counts rather than rates because of the inability to produce accurate total population estimates for each police radio zone. As figure 1 shows, police radio zone boundaries are smaller than neighborhood boundaries, which means that any population estimate derived from neighborhoods would overestimate the population within each radio zone.

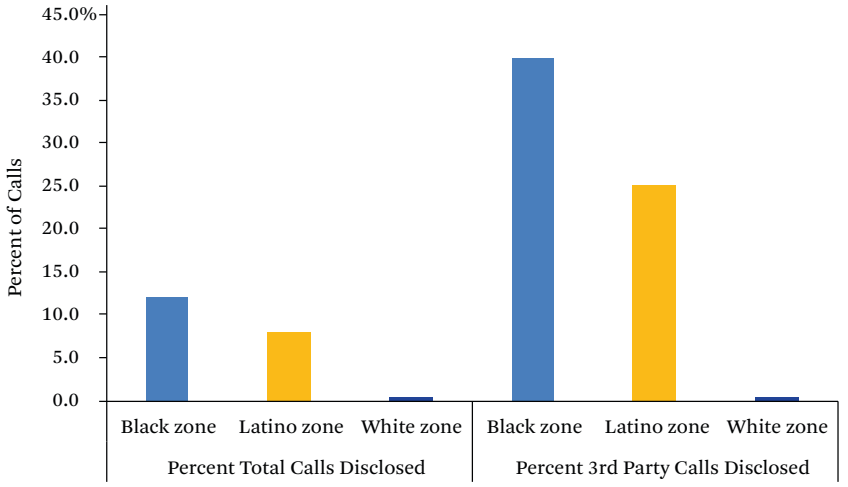
FINDINGS

The disclosure of identifiable information about callers over the radio occurred when dispatchers or officers stated a caller's first name, last name, or home address. Consider the following example:

> Case 278 in the Black Radio Zone
> DISPATCHER: Suspicious car with occupants. 2116 West State. Dana says that a red and silver car, 4-door, several occupants, male and female, parked outside of her house, and they have been there for a while.

In this call, the dispatcher disclosed the caller's first name. Although it is unclear whether 2116 West State is Dana's address, the dispatcher provides the caller's approximate home address when saying the suspicious car's occupants are parked outside Dana's house. Outside parties interested in identifying and re-

Figure 2. Total Calls and Third-Party Calls that Disclose Identifiable Information



Source: Authors' calculations.

taliating would only have to find a woman named Dana near the address of 2116 West State. At other times, dispatchers were more explicit when disclosing a caller's address.

> Case 115, Latino Radio Zone
> DISPATCHER:Person wanted at 4700 S. Chester. Diana Rodriguez is calling from 4872 Washington Street. She says a male is wanted, and that he was at that address.

In case 115, the dispatcher provides the full name and home address of a caller informing the police of the location of a man wanted by police. This disclosure renders the caller especially vulnerable to retaliation, as the consequences of her call may result in jail time for the wanted criminal. Moreover, if the caller's tip is not true, any criminal or friend of a criminal listening would know that Diana Rodriguez provides information to police on wanted suspects.

> Case 298 in the Latino Radio Zone
> DISPATCHER: There is a criminal damage to property in progress at 2543 S. May, where James was calling. Says that there is a male trying to remove a boot from an unknown vehicle. He has no other information. Although we are trying to reach him on the radio.

Case 298 is another example of dispatchers disclosing identifiable information about a citizen making a third-party call. In contrast to other calls that reference a block such as 2500 S. May, the dispatcher gives an exact address (2543 S. May). These select cases exemplify the types of third-party calls that we quantify and analyze in the following section. Findings reveal stark patterns about each police radio zone as well as the kind of crimes reported to police that are likely to result in caller identities being disclosed.

Quantitative Results

Figure 2 illustrates descriptive statistics from the two measures of digital vulnerability in each police radio zone. If we use the total number of calls as the denominator, 12 percent disclosed identifiable information in the black zone (forty-four of 371) relative to 8 percent in the Latino zone (eleven of 148) and 0 percent in the white zone (total of 131). This means that, in the black and Latino zones, approximately one of every ten calls reveals an identifiable piece of information about the caller. Even further, this means that 2.2 caller identities are disclosed per hour in the black zone and 0.55 per hour in the Latino zone.

Focusing on third-party calls illuminates more troubling findings. Forty percent in the black zone (forty-four of 111) and 25 percent in

the Latino zone (eleven of forty-four) revealed identifiable information about callers. These figures signified that black and Latino citizens had greater digital vulnerability than whites and were at greater risk of retaliation.

Examining variation in digital vulnerability by type of crime across each zone reveals more detailed findings. Figure 3 provides a breakdown of the crime type reported by the caller. It also breaks down calls by zone and whether they were third-party calls or direct-assistance calls. Figure 3 illuminates the importance of distinguishing between calls for direct assistance and third-party calls given that, understandably, to receive assistance as soon as possible, victims of domestic abuse or batteries in progress should have their names and home addresses disclosed to police.

Looking exclusively at third-party calls, however, reveals a different pattern. In the black zone, dispatchers disclosed identifiable information especially of citizens reporting batteries, gang disturbances, noise complaints, and shots fired. Relative to Latinos and whites, citizens reporting crimes on people carrying guns or knives had their identities disclosed at by far the highest rate (27 percent). This might reflect the higher number of people carrying weapons in these areas, or a higher chance that dispatchers reveal more information about callers when discussing weapons-related crimes on radio frequencies. Because a call about weapons is an especially dangerous one for the police officers investigating it, dispatchers may want to give as much information to the police as possible out of concern for officers' safety.

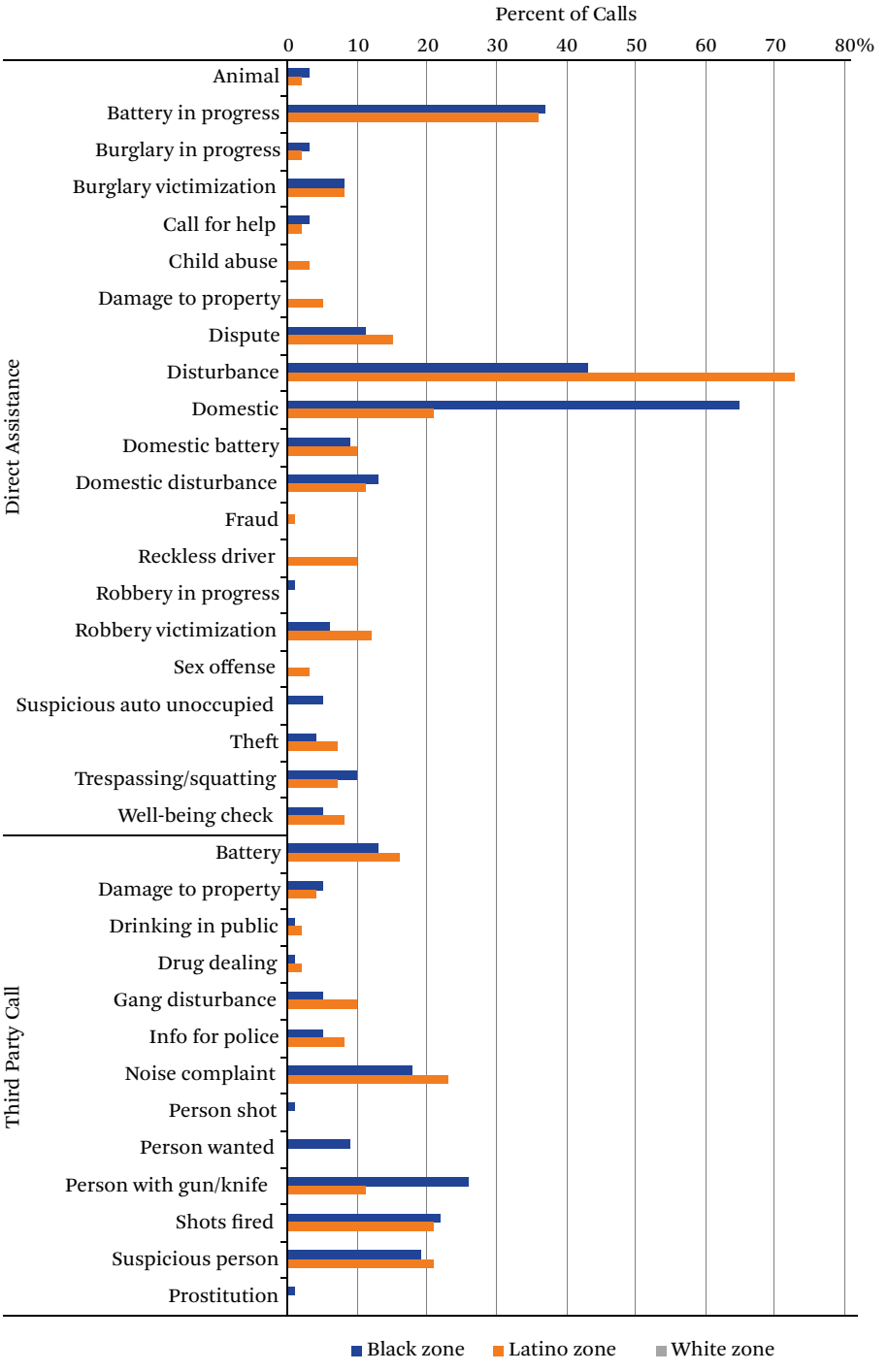
In the Latino zone, dispatchers disclosed identifiable information for citizens reporting noise complaints and suspicious persons. It makes sense for these crime types to be common among third-party calls, given that they are crimes a citizen is likely to observe by being in a public space or looking out on the street from a window. In addition, 911 dispatchers are required to ask for the name and address of the caller for police to follow up if necessary (Preusse and Gibson 2016). Interestingly, in both black and Latino zones, dispatchers do not reveal identifiable information about crimes typically associated with organized criminal groups or the informal economy. Fewer than 5 percent of calls reporting prostitution, drug dealing, or gang disturbances revealed identifiable information about the caller. This might reflect dispatchers being careful with caller's information, or the fact that few citizens even report these crimes in the first place.

Figure 4 displays data exclusively from third-party calls but groups them by the kind of identifiable information revealed and radio zone. The figure reveals that first and last names account for a larger proportion of identifiable information disclosed by dispatchers than home addresses. This suggests that, in most cases, criminals eavesdropping to identify "snitches" deduce caller identities by names and crime locations. Identifying a caller based on this limited information, according to gang ethnographers, would not be difficult because gangs tend to be adeptly aware of the community members within their territories (Sanchez-Jankowski 1991; Vargas 2016; Venkatesh 2006). Gangs inquire through family members, friends, or surrogates at community policing meetings to learn the names of neighbors who call police. On identifying callers, gangs may coerce residents into refraining from calling police again using strategies ranging from bribery to violent retaliation.

Figure 4 also illuminates some interesting racial differences. The black radio zone not only had the highest percentage of calls disclosing first and last names, it was also the only zone where dispatchers gave away callers' home addresses. Not a single caller home address was disclosed in the white or Latino zone. This finding illuminates a wide disparity in digital vulnerability across communities: African Americans were far more vulnerable to data breaches over police radio zones than any other group. It is also important that in both figure 3 and figure 4, not a single call in the white zone disclosed any piece of identifiable information about the caller.

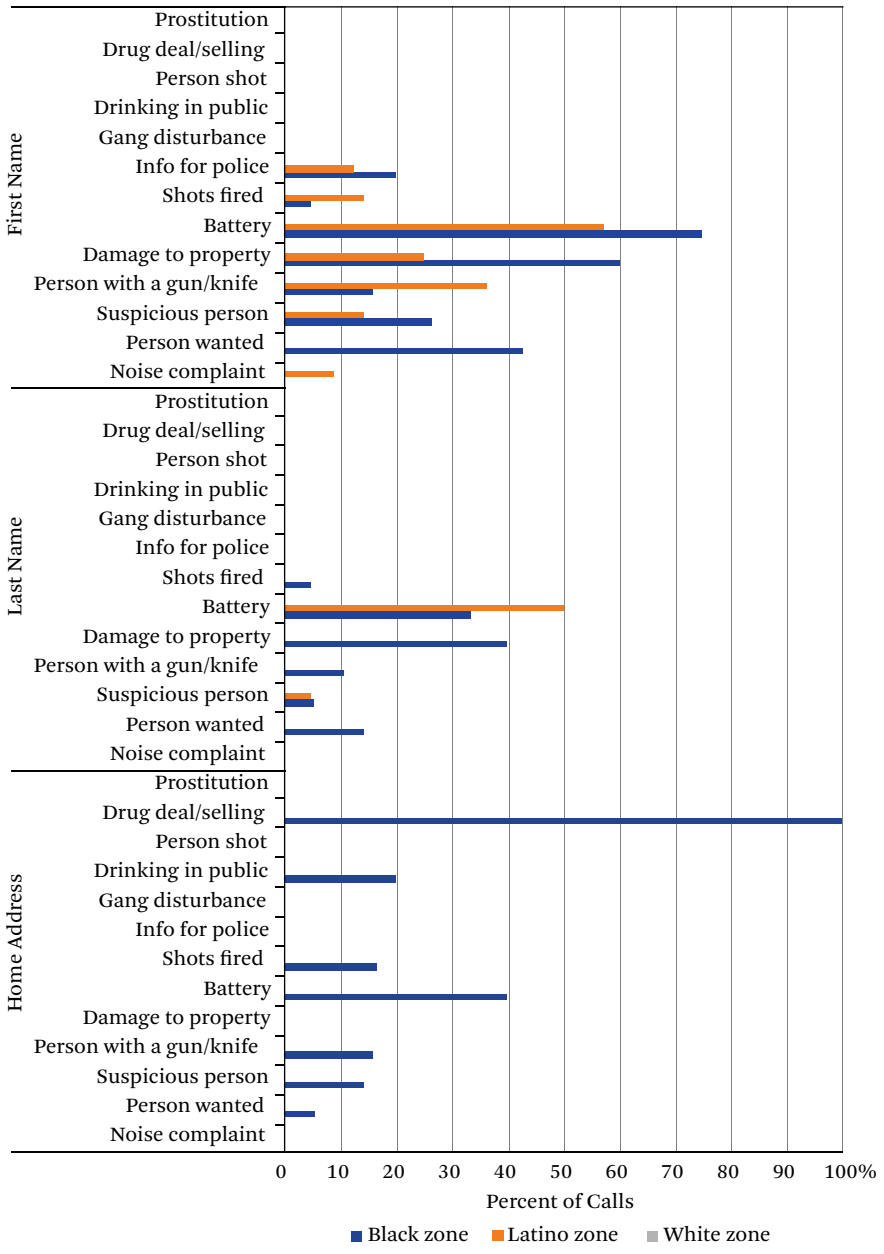
To gain further insight on factors driving differences across districts, we ran four logistic regression models displayed on table 2. Models 1, 2, and 3 predict the probability of the police reporting the first name, last name, and home address of the caller. Model 4 predicts the probability of reporting at least one of these three pieces of identifiable informa-

Figure 3. Disclosed Calls by Call Type and Crime Type



Source: Authors' calculations.

Figure 4. Disclosed Calls by Identifiable Information



Source: Authors' calculations.

tion. Each of the models contains the same independent variables for radio zone, the white radio zone being the reference category, and type of call, and public disorder calls the reference category. Public disorder calls involved less serious crimes such as noise complaints, public disturbances, suspicious persons, suspicious automobiles, reckless drivers, and public drinking.

With respect to police radio zones, the models show no significant differences between zones on the probability of reporting callers' last names. The Latino and black zones, however, disclose callers' first name and home ad-

Table 2. Logistic Regression Models: Probability of Reporting Different Kind of Information

	Model 1 First Name		Model 2 Last Name		Model 3 Home Address		Model 4 At Least One Piece of Information	
	Coef.	AME	Coef.	AME	Coef.	AME	Coef.	AME
District (ref = district 18)								
District 3	1.077*	0.154**	0.329	0.022	0.278	0.026	1.093**	0.164***
	(0.554)	(0.062)	(0.765)	(0.045)	(0.652)	(0.058)	(0.515)	(0.064)
District 6	1.148**	0.166***	0.842	0.068	1.214*	0.144**	1.554***	0.253***
	(0.555)	(0.063)	(0.757)	(0.046)	(0.642)	(0.060)	(0.514)	(0.065)
Type of call (ref = disorder)								
Intelligence	0.360	0.058	0.784	0.040	1.232***	0.148**	0.750**	0.147*
	(0.412)	(0.071)	(0.684)	(0.043)	(0.448)	(0.068)	(0.368)	(0.080)
Violent	0.465**	0.077**	1.265***	0.081***	0.575**	0.054**	0.696***	0.135***
	(0.215)	(0.036)	(0.379)	(0.023)	(0.292)	(0.027)	(0.200)	(0.039)
Property	0.931***	0.173***	1.619***	0.122***	1.394***	0.176***	1.312***	0.280***
	(0.307)	(0.063)	(0.473)	(0.047)	(0.371)	(0.057)	(0.294)	(0.066)
Domestic	2.312***	0.501***	2.180***	0.210***	3.013***	0.536***	2.988***	0.619***
	(0.259)	(0.050)	(0.390)	(0.042)	(0.302)	(0.050)	(0.303)	(0.044)
Constant	−2.630***		−3.874***		−3.215***		−2.609***	
	(0.556)		(0.792)		(0.657)		(0.517)	
Observations	650		650		650		650	

Source: Authors' calculations.
Note: Coef. = Coefficients. AME = Average Marginal Effect.
*$p < .1$; **$p < .05$; ***$p < .01$

dresses at a significantly higher rate than the white zone. A call made in the Latino police radio zone has a 16.4 percent higher probability of disclosing identifiable information, and one made in the black zone has a 25.3 percent higher probability, both relative to the white zone.

Across all four models, calls reporting domestic violence had the highest probability of disclosing first names (50.1 percent), last names (21 percent), home addresses (53.6 percent), or at least one piece of identifiable information (61.9 percent) relative to public disorder calls. Calls reporting property crimes such as trespassing, squatting, damage to property, burglary, and property theft had the second highest level of probability of disclosing identifiable information across all four models. Intelligence calls involving instances where callers had intelligence for police on wanted persons and violent calls involving persons shot, kidnappings, robberies, batteries, and people carrying guns, also had significantly higher probabilities of disclosing all types of information, but with smaller probabilities than domestic and property calls.

Model results confirm that dispatchers most frequently disclose identifiable information during direct-assistance calls for domestic violence and third-party calls involving property crime. Third-party calls on violent crimes or intelligence were less common but still significantly more likely to reveal identifiable information than public disorder calls. Overall, findings show that police radio chatter reveals identifiable information about callers at a troubling rate. Moreover, findings show substantial racial inequality as dispatchers disclosed information about callers in black and Latino neighborhoods but no information about callers in white neighborhoods.

MAKING SENSE OF UNEQUAL DIGITAL VULNERABILITY

All dispatchers serving Chicago work from a central hub station in the West Loop neighborhood that field calls for police, fire, and medical emergency services from throughout the city. Each dispatcher is assigned a zone or an area in which they take calls. Informal interviews with dispatchers suggest four factors that could help explain our findings. The first is a lack of resources to adequately staff Chicago's 911 dispatch system. In 2016, a report by Chicago's Office of Emergency Management found that 49 percent of the city's 911 emergency call takers are absent on any given day, which leaves the rest of the operators overrun with work. All 911 dispatchers qualify for the Family and Medical Leave Act, which permits employees up to twelve weeks of unpaid time off work. Advocates of 911 dispatchers argue that such time off is essential to the mental health of dispatchers, who have higher rates of depression, anxiety, and post-traumatic stress disorder (Pierce and Lilly 2012). Even worse, to address staff shortages, supervisors force dispatchers to work overtime, sometimes up to sixty hours a week. In fact, one Chicago dispatcher earned $91,000 worth of overtime pay in 2016; his base salary was $77,784 (Sargent 2013). The city government's underfunding of dispatchers, coupled with the trauma of the job, has created an environment where dispatchers are extremely overworked. In such work conditions, it is reasonable to expect mistakes to be made.

The second possible factor contributing to our results are the lax rules governing dispatcher conduct. According to the Office of Emergency Management & Communications in Chicago, rules protecting the release of callers' names and addresses over public radio frequencies are limited. Protocol instructs dispatchers to ask callers if they would like to request anonymity, but it is not a requirement. Protocol also does not discipline dispatchers for revealing identifiable information about callers. In fact, the Chicago Police Department website instructs citizens to "inform the call taker if you do not want your name given to responding police units." Thus, the burden of choosing whether to remain anonymous is on citizens, not dispatchers.

A third factor is dispatchers' well-intentioned desire to help. Conversations with three dispatchers in Chicago with whom we shared our findings revealed that during most calls dispatchers are simply trying to provide as much information to the police as possible. One dispatcher explained that revealing a caller's address happens because "you want to get that

call out to as many people as possible." The dispatchers we spoke to were hesitant to provide more detail on their firsthand experiences.

In 2016, however, a journalist interviewed a Chicago dispatcher in-depth and found that the intense trauma dispatchers hear makes them want to help callers as much as possible, and that this can often translate into providing caller information. Yana Kunichoff writes that "the dispatchers say their jobs are often misunderstood, and the criticisms levied against them are misguided at best. Their work is performed in a constantly tense environment, using a complicated and demanding technological system, under the looming threat of budget cuts" (2016, n.p.). Our inquiry into the workings of 911 dispatch in Chicago suggest that an underfunded and inadequately staffed emergency management office bears much of the responsibility for the findings in our study.

Fourth, neighborhood conditions also matter. Police officers in black and Latino neighborhoods have a significantly higher number of calls for service related to violent crimes, which may overburden dispatchers or police officers and make them prone to mistakes (Klinger 1997; Vargas 2016). Similarly, the low rates of violent crime in Chicago's white neighborhoods, which tend to be more affluent, such as the white zone in this study, make it less likely for 911 dispatchers to disclose identifiable information about white callers. Perhaps if we included a low-income white neighborhood in the study, the racial differences in our findings would have been less dramatic. Such a comparison, however, would be impossible because Chicago lacks a low-income white community comparable to black or Latino low-income communities.

It is likely that a combination of these four factors contributes to the inequality in digital vulnerability across the three radio zones. An overworked and severely mentally stressed workforce coupled with high volumes of calls from high-crime neighborhoods produces the conditions generating racially stratified digital vulnerability in Chicago.

CONCLUSIONS

In this article, we examine police-dispatcher radio communication, an older, simple, and frequently used technology, to introduce the concept of digital vulnerability for measuring inequality in citizens' risk of personal data disclosures by government agencies. Our findings suggest digital vulnerability, with respect to 911 calls for police assistance, is a real concern, especially in low-income, high-crime, minority neighborhoods. Although many residents of such communities come into contact with the criminal justice system through police stops or arrests, millions more have indirect e-contact through emergency 911 calls for police assistance, and the information conveyed in these interactions is being dangerously disclosed over public radio frequencies. This finding has several scholarly and policy implications.

First, studying digital vulnerability can illuminate inequalities generated by technologies that remain largely hidden because of the dearth of research on citizen e-contact with the criminal justice system. In the case of police-dispatcher communication, growth in low-cost smartphones and wireless internet access has made it easier for criminals to monitor police radio communication. Broadcastify.com, the website that broadcasts the Chicago Police Department's radio frequencies, averages nearly thirty thousand listeners per day. Although it is impossible to determine exactly how many individuals are listening to police scanner chatter for malicious purposes, it only takes a small portion of the thirty thousand to inflict sizable damage to police-community relations by retaliating against a caller. For example, Matthew Desmond, Andrew Papachristos, and David Kirk show that a single event such as the police beating of Frank Jude can contribute to a net loss of twenty-two thousand calls for 911 emergency service (2016). More research, however, is needed to understand the degree to which disclosing identifiable information about callers over police radio frequencies leads to violent retaliation. Nevertheless, our findings establish that the disclosure of caller information over police radio frequencies should be a concern to scholars and policymakers concerned with improving relationships between police and minority communities. Individuals' refusal to report crimes or cooperate with police investigations may stem not only from reluctance to inform on a friend or family member but also

from police and dispatchers' inability to protect caller identities.

Second, our findings show the importance of studying third parties who broker contact between citizens and agents of the criminal justice system. Our case study focused on 911 dispatchers, but lawyers (Van Cleve 2016), social workers (Stuart 2016), tax preparers (Sykes et al. 2015), and health-care staff (Lara-Millán 2014) are also occupations that share information about citizens to government bodies via digital platforms. How do these third parties safeguard private information about citizens? More research is needed on the complicated bureaucratic layers of interaction between citizens and the state, and the degree to which sensitive information may be vulnerable to exploitation.

Scholars also need to consider the digital platforms in which citizen contact with the criminal justice system occurs. Much scholarly attention has been paid to physical police stops or, in our case study, 911 calls over radio frequencies. Other forms of contact, however, occur on Facebook, Twitter, or film footage from surveillance cameras or police body cameras. To better understand the consequences of e-contact with the criminal justice system, the field sites and social contexts in which scholars observe need to evolve and incorporate cell phone usage, email usage, and data security systems. The notion of digital vulnerability, introduced in this article, can help scholars identify and measure inequalities produced from digital forms of criminal justice contact.

Finally, the article offers several policy implications for the 911 dispatch system in Chicago and possibly other cities. First, findings suggest the need to fund and adequately staff the 911 emergency system in Chicago. Given the austere financial situation of U.S. cities, funding these agencies is probably easier said than done. Nevertheless, our findings at minimum suggest that dispatchers need to be far more careful with sharing caller information. Although it makes sense for dispatchers to provide police identifiable caller information when direct assistance is needed, dispatchers need to recognize that third-party callers do not need to be identified, especially when criminal groups listen to identify and retaliate against callers. Training dispatchers to recognize the difference between direct-assistance calls and third-party calls may decrease digital vulnerability in black and Latino communities.

Some may argue that our findings suggest the need for police departments to scramble their radio frequencies, which would prevent any third party from listening. We would caution any reader from drawing this conclusion. Cities such as Washington, D.C., and Santa Monica have already taken their police radio frequencies offline (Hudson 2011), but no evidence suggests that this has improved police-community relations, officer safety, or citizen calls for service. The debate between government transparency on the one hand and the need for security on the other is real and important. However, research remains scant on this issue and policymakers should not rush to conclusions. At the moment, we contend that simply training 911 dispatchers to be more discreet when sharing identifiable information about third-party callers should help reduce digital vulnerability. Hastily scrambling police radio frequencies may result in an unnecessary trade-off between the Democratic value of government transparency and citizen security.

REFERENCES

Asher, Jeff, and Rob Arthur. 2017. "Inside the Algorithm That Tries to Predict Gun Violence in Chicago." *New York Times*, June 13. Accessed September 8, 2018. https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html.

Brayne, Sarah. 2014. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." *American Sociological Review* 79(3): 367–91.

———. 2017. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82(5): 977–1008.

Chicago Crime Commission. 2012. *The Gang Book*. Chicago: Cook County Crime Commission.

City of Chicago Data Portal. 2016. "Crimes 2001–Present." Accessed July 1, 2016. https://data.cityofchicago.org/Public-Safety/Crimes-2001-to-present/ijzp-q8t2.

City of Chicago Radio Communications. 2016. "General Order G03-01-01." Chicago Police Department. July 13. Accessed September 17, 2018.

http://directives.chicagopolice.org/directives/data/a7a57be2-128ff3f0-ae912-8ff7-442a6e5fde43e2df.html.

Davis, Julie. 2015. "Hacking of Government Computers Exposed 21.5 Million People." *New York Times*, July 9. Accessed September 8, 2018. https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

Desmond, Matthew, Andrew V. Papachristos, and David S. Kirk. 2016. "Police Violence and Citizen Crime Reporting in the Black Community." *American Sociological Review* 81(5): 857–76.

Federal Bureau of Investigation. 2013. "Crime in the United States: Uniform Crime Reports for the United States 2012." Washington: U.S. Department of Justice.

Federal Communications Commission. 2008. "The Public and Broadcasting." Washington: The Media Bureau. Accessed September 17, 2018. https://www.fcc.gov/sites/default/files/public-and-broadcasting.pdf.

Fineman, Martha Albertson. 2008. "The Vulnerable Subject: Anchoring Equality in the Human Condition." *Yale Journal of Law & Feminism* 20(1): Article 2. Accessed September 8, 2018. https://digitalcommons.law.yale.edu/yjlf/vol20/iss1/2.

Gambetta, Diego. 1996. *The Sicilian Mafia: The Business of Private Protection*. Cambridge, Mass.: Harvard University Press.

Hagedorn, John. 2015. *The Insane Chicago Way: The Daring Plan by Chicago Gangs to Create a Spanish Mafia*. Chicago: University of Chicago Press.

Hudson, Travis. 2011. "Police Departments Encrypting Radio Traffic as Scanner Technology Proliferates." *Dallas News*, November 21.

Invisible Institute. 2016. "Citizens Police Data Project." Accessed July 1, 2016. https://cpdp.co/.

Jacobs, James B. 2015. *The Eternal Criminal Record.* Cambridge, Mass.: Harvard University Press.

Jacobs, Bruce A., and Richard Wright. 2006. *Street Justice: Retaliation in the Criminal Underworld*. Cambridge: Cambridge University Press.

Kirk, David S., and Andrew V. Papachristos. 2011. "Cultural Mechanisms and the Persistence of Neighborhood Violence." *American Journal of Sociology* 116(4): 1190–233.

Klinger, David A. 1997. "Negotiating Order in Patrol Work: An Ecological Theory of Police Response to Deviance." *Criminology* 35(2): 277–306.

Kunichoff, Yana. 2016. "Why Are Half of Chicago's 911 Operators Absent from Work?" *Chicago Magazine*, October 21. Accessed September 8, 2018. http://www.chicagomag.com/city-life/October-2016/911-call-takers.

Lageson, Sarah. 2016. "Found Out and Opting Out: The Consequences of Online Criminal Records for Families." *Annals of the American Academy of Political and Social Science*. 665(1): 127–41.

Lara-Millán, Armando. 2014. "Public Emergency Room Overcrowding in the Era of Mass Imprisonment." *American Sociological Review* 79(5): 866–87.

Manza, Jeff, and Christopher Uggen. 2008. *Locked Out: Felon Disenfranchisement and American Democracy*. Oxford: Oxford University Press.

Massoglia, Michael, and William Alex Pridemore. 2015. "Incarceration and Health." *Annual Review of Sociology* 41: 291–310.

NENA. 2017. "911 Statistics." Accessed September 8, 2018. https://www.nena.org/?page=911Statistics.

Pager, Devah. 2003. "The Mark of a Criminal Record." *American Journal of Sociology* 108(5): 937–75.

Paquette, Danielle. 2015. "Why Some Police Departments Let Anyone Listen to Their Scanner Conversations—Even Criminals." *Washington Post*, December 4.

Patrick, Robert. 2014. "St. Louis Police Encrypting Radio to Foil Listeners." *St Louis Post-Dispatch*, October 10.

Pierce, Heather, and Michelle M. Lilly. 2012. "Duty-Related Trauma Exposure in 911 Telecommunicators: Considering the Risk for Postraumatic Stress." *Journal of Traumatic Stress* 25(2): 211–15.

Preusse, Kimberly C., and Christina Gipson. 2016. "Dispatching Information in 911 Teams: A Case Study." In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60. Los Angeles: SAGE Publications.

Sanchez-Jankowski, Martin. 1991. *Islands in the Street: Gangs and American Urban Society*. Berkeley: University of California Press.

Sargent, Jordan. 2013. "The Chicago City Employee That Made $91,000 in Overtime in 2012 Has Things Figured Out." *Gawker*, January 22. Accessed September 8, 2018. http://gawker.com/5978182/the-chicago-city-employee-employee-that-made-91000-in-overtime-in-2012-has-things-figured-out.

Serrato, Jacqueline. 2017. "Ice Raids Could Crack Down on Mexican-American Gangs in Chicago." *Chicago Tribune*, July 24.

Sewell, Abigail A., and Kevin A. Jefferson. 2016. "Collateral Damage: The Health Effects of Invasive Police Encounters in New Yok City." *Journal of Urban Health* 93(1): 42–67.

Shane, Scott, Nicole Perloth, and David E. Sanger. 2017. "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core." *New York Times*, November 12.

Soss, Joe, Richard C. Fording, and Sanford Schram. 2011. *Disciplining the Poor: Neoliberal Paternalism and the Persistent Power of Race*. Chicago: University of Chicago Press.

Stuart, Forrest. 2016. *Down, Out, and Under Arrest: Policing and Everyday Life in Skid Row*. Chicago: University of Chicago Press.

Sugie, Naomi F. 2015. "Chilling Effects: Diminished Political Participation Among Partners of Formerly Incarcerated Men." *Social Problems* 62(4): 550–71.

Sugie, Naomi F., and Kristin Turney. 2017. "Beyond Incarceration: Criminal Justice Contact and Mental Health." *American Sociological Review* 82(4): 719–43.

Sykes, Jennifer, Katrin Kris, Kathryn Edin, and Sarah Halpern-Meekin. 2015. "Dignity and Dreams: What the Earned Income Tax Credit Means to Low-Income Families." *American Sociological Review* 80(2): 243–67.

Turney, Kristin. 2014. "Stress Proliferation Across Generations? Examining the Relationship Between Parental Incarceration and Childhood Health." *Journal of Health and Social Behavior* 55(3): 302–19.

U.S. Census Bureau. 2016. "Summary File." 2010–2015 American Community Survey. Washington: U.S. Census Bureau.

Van Cleve, Nicole Gonzalez. 2016. *Crook County: Racism and Injustice in America's Largest Criminal Court*. Stanford, Calif.: Stanford University Press.

Vargas, Robert. 2016. *Wounded City: Violent Turf Wars in a Chicago Barrio.* New York: Oxford University Press.

Venkatesh, Sudhir Alladi. 2006. *Off the Books*. Cambridge, Mass: Harvard University Press.

Vuolo, Mike, Sarah Lageson, and Chris Uggen. 2017. "Criminal Record Questions in the Era of 'Ban the Box.'" *Criminology and Public Policy* 16(1): 139–65.

Wakefield, Sara, and Christopher Wildeman. 2013. *Children of the Prison Boom: Mass Incarceration and the Future of American Inequality*. Oxford: Oxford University Press.