



The Journal of Civic Information

Volume 5 | Number 3

November 2023

Journal homepage: <https://journals.flvc.org/civic/>

ISSN (online): 2641-970X

Owning the Police: Crime Data, Copyright, and Public Information

A.Jay Wagner *

Article Information

Received: May 17, 2023

Accepted: June 26, 2023

Published: November 30, 2023

Keywords

Freedom of information
Government transparency
Police records
Crime data
Copyright

Abstract

Online crime maps, which plot law enforcement crime data, promise to promote civic engagement and increase government transparency. This study reviewed the websites of the 250 largest U.S. cities and found 65% host or link to a crime map, and that 116 police departments entered into agreements with crime mapping companies that provide the companies preferred or exclusive access to local crime data, curtailing public access and use. This study examines the legal tactics used by commercial mapping companies to maintain information control, explores recent examples of legal battles over the data, and proposes solutions, including targeted public record law amendments, parallel access, and a generalized right of access.

* A.Jay Wagner, Ph.D., is an associate professor in the Marquette University Diederich College of Communication. This manuscript won third place in the National Freedom of Information Coalition 2022 freedom of information research competition, presented October 19, 2022. Please send correspondence about this article to A.Jay Wagner at ajay.wagner@marquette.edu.

To cite in Bluebook: A.Jay Wagner, *Owning the Police: Crime Data, Copyright, and Public Information*, 5 J. CIVIC INFO. 3, 1-16 (2023).

To cite in APA: Wagner, A.J. (2023). Owning the police: Crime data, copyright, and public information. *Journal of Civic Information*, 5(3), 1-16.

DOI: 10.32473/joci.5.3.134941

Published under Creative Commons License CC BY-NC, Attribution NonCommercial 4.0 International.

Introduction

In 2010, Public Engines, a company that published online crime maps, filed a lawsuit against Reportsee, another online crime mapping company. Both commercial companies relied on maps that plotted law enforcement crime data (*i.e.*, details on incidents or calls for service). Despite the crime data being public information, Public Engines essentially sued Reportsee for stealing their data. A visitor to either crime mapping company's website would not have noticed much difference between the two, but the companies operated quite differently. Public Engines developed and sold proprietary software to law enforcement agencies. Police departments and sheriffs' offices used the software to compile incident-level crime data for internal tracking and analysis. In selling the software to local law enforcement agencies, the parties would frequently enter into a concurrent agreement to plot the crime data to their public website, CrimeReports. Reportsee mapped similar crime data but without the proprietary software or preferred access. They were more opportunistic in seeking crime data. In some instances, law enforcement agencies proactively posted crime data to their website, which Reportsee gladly accessed. Other times, they submitted freedom of information (FOI) requests or made informal asks for crime data. The two companies' business models differed, as well. Public Engines made the bulk of its revenue in selling software, and Reportsee generated revenue by selling advertisements on their website, SpotCrime.

The suit stemmed from Reportsee scraping—extracting website data using a bot or web crawler—their competitor's website, because law enforcement entities had informed them Public Engines was their mapping provider and was either the exclusive or preferred recipient of crime data. When Reportsee's informal appeals and FOI requests for equal access produced no remedy, they resorted to scraping the crime data. The parties would come to an agreement prior to a court decision with Reportsee agreeing to cease scraping Public Engines's website and no longer publish Public Engines's crime report data.

The outcome was confounding for several reasons. First, crime data is indisputably public information. There are colorable arguments that crime data in some instances may not meet the statutory definition of an existing record—a requirement in most FOI laws—but if a government entity is distributing the crime data to one party, then it would seem inequitable to refuse to distribute it in the same fashion to another party. Second, some law enforcement agencies would refer citizens to the Public Engines's website as the legal and official location of crime data. However, Public Engines had no responsibility to distribute the data to citizens. The result was a commercial company receiving preferred or exclusive access to crime data, and sometimes even claiming ownership of the data. The company now effectively controlled the crime data, and any other party was now required to use the crime data on the company's terms. Law enforcement entities enter these public-private agreements for various reasons, but a primary motivation is in controlling the flow of the information (Wisnieski, 2014). Generally, the commercial agreement and existing financial relationship makes the commercial entity a trusted partner. One metro police department defended not sharing crime data with the public, but with a commercial mapping company, over concerns of accuracy and not wanting to confuse the public with multiple sources of information (Wisnieski, 2014). The commercial entities enter these agreements because there is value in crime data. Whether it enhances the worth of their products, drives traffic to their website or burnishes the company's image, there is discernible financial value in owning crime data, especially if it can be collected at scale. In most jurisdictions, there is no explicit statutory or administrative requirement to distribute the incident-level crime data that appears in the maps, and,

as mentioned above, the private companies have no such responsibility, either. However, all law enforcement entities are subject to FOI laws, and the arrangement between crime mapping companies and law enforcement entities circumvents FOI laws. By granting direct access to the crime database, law enforcement agencies claim the data are not an existing record (as the data are information in software and not an output) or direct those interested in crime data to the commercial crime mapping website, where the companies have intentionally degraded the quality of the data (*e.g.*, removing or generalizing categories of information), intentionally undercut usability (*e.g.*, disabling copy-pasting or not allowing for downloading of the data) or erected legal barriers to using the data (*e.g.*, prohibitive terms of use, including disallowing commercial use).

This favoritism contradicts first-order principles of equitable access to government information and effectively allows law enforcement agencies to pick winners and share valuable crime data with only preferred parties. Distributing crime data to one party, while outright refusing to provide the same data to another party or offering a lesser or degraded form of the data, is fundamentally wrong. As a government, such bias without a reasonable justification conflicts with foundational connotations of equality and due process. Equity in access is fundamental to many key access to information efforts, like FOI laws. For this very purpose, many FOI laws prohibit consideration of the requester's identity or the requester's purpose for submitting a request to ensure that access to government information is free of favoritism or partiality. Further, there is no rationale for limiting the circulation. The utility of its original distribution only grows when more individuals are given access, and the beneficiary to restricting distribution to one commercial entity is accrued solely by that commercial entity. No public good results from allowing the single company to gain control of the information. Yet, the practice of preferencing commercial access over public access continues. Some of the names in crime mapping have changed (*e.g.*, Public Engines was bought by telecom behemoth Motorola in 2015), but the disregard for fair and equitable public access has not. The government outsourcing of records and data administration has grown, and Spivack (2017) documented other instances where local governments have ceded control of information to commercial entities. In New York, California, and Missouri, same-day access to court documents—a long-standing right—ceased due to new digitization processes and a new insistence on privacy. Georgia's official state laws have been subject to an ownership dispute due to the company responsible for publishing the laws adding notes to the state code. Government building ordinances are commonly published by local jurisdictions but adapted to a useable format by trade organizations who turnaround and sell access to the public.

In surveying the status of crime maps in the United States, the author of this study found crime mapping to be common among law enforcement websites. This study found 65% of the 250 largest U.S. cities' police departments host or link to a crime map on their website, and nearly half of the 250 police departments used a commercial mapping service with prohibitive features or restrictive terms of use. The following manuscript proposes a reevaluation of the practice of providing commercial entities with exclusive or preferred access to government information. First, the manuscript reviews the literature on crime mapping and government data issues, followed by a survey of the present status of crime data in the United States. Then, the manuscript examines the major commercial players in crime mapping and their legal positions, followed by a review of relevant legal cases, including some recent federal cases that further suggest reevaluating access to crime data. The manuscript concludes by calling for equitable access and proposes solutions to the problem.

Literature review

Scassa (2016) defined geolocated crime data as, “Publicly accessible crime maps offer[ing] an interactive visual display of criminal activity within a municipality. Typically, they display multiple categories of crime plotted according to time and geographic location” (13). Chainey and Thomson (2012) observed crime maps generally aim to increase law enforcement credibility, reassure the public, promote dialogue between law enforcement and the public, and ultimately foster democratic transparency. Wallace (2009) offered a broad critique of the practice. She argued publishing crime statistics is an advertisement for the effectiveness of law enforcement, both justifying their work and acting as an implicit ask for further commitment and resources. The maps, Wallace wrote, “conjure the perfectly efficient and omniscient police forces now common on police procedurals on television ... in which all data are known or knowable, and from it, impeccably trained experts find solutions and reach the right conclusions in a timely manner” (p. 20). Wallace expressed concern about the larger implications, calling crime mapping ultimately an exercise in power and faulty in putting forward the impression that this is a complete and comprehensive view of the neighborhood’s criminal activity, reducing crime to a simple and straight-forward problem, instead of complex social issues.

Chainey and Tompson surveyed crime mapping in the United Kingdom, which mandated nationwide crime mapping in 2011. They concluded their survey by suggesting none of the goals of crime mapping were being met, adding witheringly that crime maps promote political transparency, not real accountability. The U.K. mapping effort was in response to a 6-year government study that found the public to be generally ill-informed about crime. The solution was to enter the conversation through dependable, visually attractive crime data. It was believed publishing crime maps would engage the public, especially on the matter of local crime and begin dialogue anew about law enforcement and crime. Chainey and Tompson, however, were unable to find any evidence that the use of crime mapping produced community engagement or empowerment. In seeking existing research that documented crime maps meeting the sought objectives, they found only two studies that contradicted each other and produced generally weak findings (Groff et al., 2005; Quinton, 2011). They found a huge initial interest in the crime maps, followed by a sharp decrease in online visitors to the pages. The duo concluded that there may be benefits to crime mapping, but as yet there remains little evidence it produces any results with consistency.

Scassa assessed the implementation of the three most popular crime mapping platforms in Canada: CrimeMapping, under the previous owner The Omega Group; RAIDS Online, the predecessor to the LexisNexis Community Crime Map; and Public Engines’s CrimeReports, since bought and shuttered by Motorola. Scassa, like other scholars, was ultimately fairly pessimistic about the impact of crime maps. She made note of the inconsistency of data across different law enforcement agencies, making cross-jurisdictional comparison—a primary selling point—unreliable. She also made special note of crimes that lack geographical dimensions. For instance, many computer and internet crimes are not especially compatible with geolocation. Similarly, many financial crimes and fraud do not lend themselves to mapping. As a result, these maps distort public perceptions of crime, focusing on specific strains of violent crime and property crime, which can reflect classist and racist tropes. Further, some communities underreport crime or are less likely to make a call for service due to trust issues with law enforcement, and this also distorts the appearance of local crime. She concluded that the crime maps scarcely meet their stated objectives and ultimately produce a very thin form of civic engagement. She called the data of relatively poor

quality, incomplete, potentially inaccurate, and presented in a way that can be confusing or misleading.

Important other considerations include conflating crime mapping efforts with established accountability measures; or, as Chainey and Tompson called it, confusing theater of transparency for meaningful accountability. Worse, crime has increasingly become entertainment (Palmer, 1998). Open government efforts, like crime mapping, are ideologically akin to bedrock transparency laws, like FOI laws, though open government should not be confused with real government access or public records laws (Schrock, 2016). And crime maps have frequently interrupted FOI laws, principally, when law enforcement attempts to offload to third parties their statutory responsibility to provide the public with access to government records.

Law enforcement transparency

The 1966 Freedom of Information Act (FOIA) codified the U.S. government's commitment to providing its citizens with access to government records. But prior to the FOIA's passage, the government had installed various mechanisms for providing the public with government information under a belief that self-governance required an informed public. Doty (2000) cataloged many of these efforts—from the 1860 founding of the Government Printing Office to the 1935 establishment of the Federal Register—the federal government has demonstrated an enduring commitment to informing the public of its activities. And since the FOIA was enacted, those in positions of power have insisted the law was a democratic imperative and that access to government information a first-order priority. Each president, save George H. W. Bush and Donald Trump, explicitly supported increased government transparency and the FOIA (Wagner, 2021a). The Supreme Court has underscored the FOIA's importance on many occasions. In a 1978 case, Justice Thurgood Marshall called the FOIA “vital to the functioning of a democratic society” (*NLRB v. Robbins*, p. 242). These laws were explicitly designed to be fair and equitable and do not consider the identity of the individual or the purpose of the request. The FOIA, which is the template for state FOI laws (which govern all subsidiary governments), explicitly requires agencies to make records “available to any person.” The Supreme Court has stated that neither requester identity nor purpose should be considered when processing a request, “withholding information under FOIA cannot be predicated on the identity of the requester ... citizens should not be required to explain why they seek the information” (*NARA v. Favish*, pp. 170-172). And with the exception of Arkansas, Delaware, Kentucky, Nebraska, Tennessee, and Virginia (which require state citizenship to make a request), identity is not to be considered in state FOI laws. Aside from fee considerations, states do not consider the purpose of the request. The Supreme Court has directly addressed favoritism in FOIA processing, “The [FOIA] clearly intended to give any member of the public as much right to disclosure as one with a special interest” (*NLRB v. Sears, Roebuck, & Co.*, 1975, p. 149). These bedrock principles exist because FOI laws were designed to further inform the public, broaden civic engagement, and generally grow equality.

Despite the repeated intimation from the highest levels of government that transparency and the FOIA are essential, there have been deficiencies in realizing the objectives of the transparency as a principle and the FOIA as a law (Fenster, 2017; Pozen, 2016). Collectively, law enforcement has proved to be a particularly challenging body in manifesting government transparency and proved to be especially vexing with regard to fulfilling the objectives of FOI laws. Law enforcement agencies have consistently scored poorly in studies of FOI responsiveness.

In a field study involving submission of 1,002 FOI requests across 334 counties, nine states, and five different government bodies, Wagner (2021b) found sheriffs' offices to have the worst performance in request outcomes, delays, and communication. Kimball (2003) found law enforcement agencies to be the most likely to withhold information requested via FOI. She cataloged law enforcement officials across several states acting with hostility toward requesters (p. 315). Kimball also reviewed 24 FOI audits and found law enforcement agencies to be the least compliant in 19 of the audits. Cuillier (2010) documented law enforcement entities frequently illegally denying or ignoring requests. In submitting a request to 104 Arizona police agencies, Cuillier received a response 48% of the time and the requested records in just 9% of the requests. While law enforcement entities have garnered a poor reputation among FOI requesters, the dynamic between police departments and sheriffs' offices and the community is multifaceted and fraught with difficult decisions (Cook & Fortunato, 2022; Ingrams, 2017).

Crime data

There are no universal requirements that law enforcement agencies publish crime statistics in the United States. Despite nearly all law enforcement entities keeping a running tally of criminal activity, many provide the public with little more than old aggregate crime statistics. Many offer the public nothing at all. The FBI encourages voluntary participation in a federal crime-tracking initiative, and many states have their own requirements, but public information regarding crime in the United States is a case-by-case scenario. Historically, the one reasonably dependable source of crime data was quarterly FBI statistics. Wilson (2002) reasoned that local criminal justice officials struggle with data collection and research, because they are too attached to the results. The lack of systematic data and research standards also limits comparison and context severely undercutting analytical value. The FBI introduced a new, richer crime data reporting standard recently. It retired its 90-year-old crime reporting program in 2021, transitioning to a new, more detailed reporting system. The older Uniform Crime Reports (UCR) system focused on aggregate data on eight crimes. The newer National Incident-Based Reporting System (NIBRS) provides significantly more information and recalibrates crime reporting around individual incidents, capturing more information about each event.

The transition between the UCR and NIBRS system also introduces an interregnum where crime statistics will weaken significantly. The FBI estimated that law enforcement agencies representing nearly 95% of the U.S. population regularly reported their statistics to the FBI under the legacy UCR system (Asher, 2022). As of summer 2022, more than 7,000 of the nation's 18,000 law enforcement agencies (agencies representing more than one-third of the U.S. population) did not make the switch and report data to the FBI (Li, 2022). Crime analysts have suggested this undermines the fidelity of the national data, and many believe this transition may muddle crime statistics for half a decade or more (Asher). Nonetheless, given the patchwork nature of crime statistics, quarterly FBI data are quite often the only information on local crime available to the public. Outside of the FBI data, law enforcement sharing of crime data is lacking. A criminal justice organization recently evaluated crime data transparency in 94 U.S. cities. In evaluating 10 categories of data transparency—including use of force reporting, publication of calls for service, sharing of complaints about police misconduct, etc.—the highest scoring city, Chicago, earned a 70 (out of 100) and only 21 of the 94 scored higher than 50 (Vera Project, 2022). The evaluation concluded that police data transparency in the United States to be very poor, and crime reports and calls for service to be among the areas most in need of improvement. Journalists have documented

a growth in public agencies outsourcing record-keeping responsibilities (Hochberg, 2013). Law enforcement agencies enter into these commercial relationships aware of the tradeoff. The Columbus Police offered a public feed with comprehensive crime data, but then entered into a commercial data and mapping agreement. Suddenly, the public feed was turned off, and public access reduced to periodic statements with fewer fields of information (Wisniewski, 2014). Similarly, in Minneapolis, upon entering a commercial agreement, two classes of crime data were produced: a feed of current data to the commercial company and monthly spreadsheets for journalists and citizens.

Crime mapping platforms

Crime maps are currently quite popular. A review of the 250 most populous cities found 65% of these cities hosted or linked to a map with crime information, and 48% of the cities used a commercial crime mapping product that presented significant restrictions to the use of crime statistics. Methodologically, the 250 cities in the United States with the largest populations, per the 2020 Census Bureau count, were first identified. All commercial mapping companies host a centralized map with the information of all participating law enforcement entities, and these centralized maps were searched for the 250 cities. Next, each city's police website was individually searched by the author for the presence of crime statistics and crime maps. In instances where both crime statistics and a crime map were not identified, the author then performed a focused internet search for city-specific crime maps. After this information was recorded and crosschecked, a FOI request was sent to each police department seeking any crime statistics or mapping contracts or agreements. The request specifically referenced contracts or agreements with the four commercial crime entities below (as well as their precursor companies), in addition to any contracts or agreements mentioning Esri or ArcGIS.

The study found five different crime maps across the 250 cities: LexisNexis's Community Crime Map, CentralSquare Technologies's CrimeMapping, Motorola's CityProtect, Corona Solutions's MyNeighborhood, and in-house platforms (see Table 1, below). The four commercial companies are dramatically different in their approaches to crime mapping and vary considerably in their size and ambitions. The sophistication of the graphic and data presentation also shows significant differences. The four companies also demonstrate distinctly different legal approaches to the crime data, ranging from MyNeighborhood's genial open access to the Community Crime Map's technical limitations and hostile legal disposition on third-party data use. In-house options also vary considerably, often according to the resources of the city's GIS departments. The in-house maps, notably, lack the financial motives, and thus offer a much different legal approach.

Table 1

Crime Maps in U.S. Cities with Largest Populations

Product (Company)	<i>n</i>	% of all cities	% of crime maps
Community Crime Map (LexisNexis)	61	24.4	37.0
CrimeMapping (CentralSquare)	45	18.0	27.3
CityProtect (Motorola)	9	3.6	5.5
MyNeighborhood (Corona Solutions)	4	1.6	2.4
In-house	46	18.4	27.9
No map	87	34.8	-
Total	252	100.0	100.0

Note. Two cities had two crime maps.

Community Crime Map

LexisNexis’s Community Crime Map was the most popular commercial product, appearing in just under one-quarter of all city pages. The Community Crime Map is operated by LexisNexis, a large data and information corporation. LexisNexis acquired the existing crime mapping product, RAIDS Online from BAIR Analytics in 2015. The Community Crime Map is the most advanced of the commercial options, providing an intuitive user experience and tabs for the crime map, as well as a data grid and analytics. The public interface was overhauled in July 2022, which is notable as the other commercial mapping services are dated in appearance and slow in operating. It is a free service for law enforcement agencies that use LexisNexis Risk Solutions products.

The Community Crime Map plots case or incident reports. Incident reports are instances where law enforcement has recorded an interaction and the potential of criminal activity has been documented. This is a step beyond calls for service though does not necessarily entail criminal charges either. In most instances, the Community Crime Map updates crime data daily. The data is easily sortable by date, geography, and type of incident. There are no search limits by date, allowing individuals to search crime data in some geographies a decade or more in the past. Notably, the LexisNexis product offers additional data features, including the underlying crime data in tabulated form, as well as some rudimentary analytics (*e.g.*, a pie chart sorting by type of crime, bar charts for days of the week and hours of the day). The Community Crime Map offers a

spreadsheet of the data, a laudable effort. However, the spreadsheet has stripped away functionality that limits its usability and as a result users cannot copy the data nor download it.

CrimeMapping

The CrimeMapping website is hosted and owned by CentralSquare Technologies, a software company with concentrated interests in data science, cloud computing, and AI. The majority of their software products serve governments. CrimeMapping was originally developed by The Omega Group, and TriTech took control of the mapping software in 2016, and then a 2018 merger resulted in the current name. Review of city contracts reveals many cities pay no additional cost for the CrimeMapping extension of CrimeView (the internal crime map interface), though a number of city's paid a small (*i.e.*, \$1,000-\$2,800) annual subscription fee.

CrimeMapping offers a less modern interface than the Community Crime Map and similar functionality; a map that can be filtered by location and date, along with a report tab and a chart tab. The report tab is a spreadsheet of the crime data with categories for incident type, incident category, incident location (block-level), and time and date. The chart feature provides a bar chart sorting by incident type and day of the week, along with a pie chart of incident types. Notably, CrimeMapping allows the user to print out the crime map, the crime report, and the crime charts. While this does not meet the standards of individuals looking to systematically analyze the crime data, it is an improvement on LexisNexis's deliberately undermining the useability of their data. CentralSquare's product, like LexisNexis, plots incident report data and typically updates each location daily. Law enforcement agencies determine how the reported incidents are coded and mapped. CrimeMapping only offers the most recent six months' worth of data. They instruct users interested in more than six months' worth of data to contact the law enforcement agency directly.

CityProtect

In 2015, Motorola acquired the aforementioned Public Engines and its mapping platform, CrimeReports, which was at the time of the transaction the most popular of the online crime maps. CrimeReports no longer exists, and instead Motorola now operates CityProtect, a crime mapping interface that is buggy and challenging to use. In 2019, Motorola effectively divested itself from crime mapping, ending its partnership with Socrata, shuttering the successful CrimeReports and launching CityProtect (Westrope, 2019). This transition ended the availability of a considerable amount of machine-readable crime data (likely more than 1,000 law enforcement agencies). Motorola sold Socrata to competitor Tyler Technologies, an aggressive player in public sector software. There is an additional cost to cities in using CityProtect, and on multiple occasions city or law enforcement officials said the expense was the reason they no longer used the service.

While only 9 of the 250 surveyed cities had functioning CityProtect pages, it was relatively common to either find a law enforcement agency's page on CityProtect that is no longer updating, or for the law enforcement agency to have a defunct link to CityProtect on its own page. The map plots incidents, though the filter function allows for the inclusion of calls for service (though this never produced additional data points on the map for the author). Most pages claimed to have been updated the day of use (though this appeared inaccurate). Oddly, the pop-up when entering the site for the first time encourages users to help solve crime. The functionality of the page accords with Motorola's flagging interest in crime mapping. It is clumsy and difficult to find the agency, and when the incidents do populate the map, there is often no information for each incident, meaning

there is a geolocated incident graphic devoid of any context. With some effort you can deduce the incident type, but this is the extent of the information available to the user. Users can filter by time, date, and incident type categories. One year's worth of data is made available.

MyNeighborhood

MyNeighborhood was found in 2% of the reviewed cities, and according to their website only have eight total law enforcement agencies actively using the service. Unlike the other commercial crime maps, MyNeighborhood plots calls for service, which is merely a law enforcement contact by an individual in the community and not necessarily criminal in any way. The data is updated daily, and the categories and definitions are determined by the interface owner Corona Solutions, a software company specializing in serving law enforcement. It is a clean and functional website, offering a calls for service map, two simple graphs, and a table of plotted points on the map. The table includes the type of call, the location, time and date, and number of cars sent. There are no limitations to functionality and copy-pasting or scraping of the data appears permissible.

In-house

A substantial number of cities, 18% of all reviewed, produced their own in-house map. The in-house maps typically use existing resources, repurposing mapping and database products. The vast majority of these in-house maps are plotted using Esri's ArcGIS, a popular mapping software licensed by many cities across the country. City or law enforcement officials have proactively chosen to tap into their existing mapping resources and plot their crime data. It is important to note that these in-house maps do not come with the limitations of the commercial options. In some cases, the interface is slow and clunky or lacks features, but, again, comes at no additional cost and does not restrict public access. In other cases, the maps are very high-quality and easy to use. Many of the open data portals proactively publish crime data in common spreadsheet and machine-readable formats. Esri ArcGIS's terms of use do grant Esri and the Esri community permission to use, reproduce and distribute (though the content owner can provide constraints). Unlike the other companies, Esri is decidedly non-proprietary in their approach to user data, and the platform encourages the sharing and reproduction of noncommercial content. Esri's ArcGIS is very popular mapping tool across many fields and industries, but they explicitly promote to law enforcement agencies a public-friendly crime data and crime mapping option (Delaney, 2020).

Legal considerations

The companies bear no legal responsibility for providing crime data to the public. The bind materializes when the public seeks this crime data, and a law enforcement agency refers the individual to the mapping company. In many instances, neither the map nor the mapping company will help in providing useable crime data. Whether the crime data itself is publicly available is another contested point. There is a colorable argument to be made that crime data does not constitute an existing record, a prerequisite of most FOI laws. In some cases, law enforcement will provide access to an API, a feed of machine-readable data, to a mapping company, and then refuse to provide the API to individuals or other companies. On many occasions, local police offered a public feed only to turn it off after entering an agreement with a commercial mapping company.

Law enforcement agencies have justified these preferential practices by claiming they do not support websites that use crime data and also run ads; while others have defended themselves by suggesting it is about controlling the data and ensuring data quality and accuracy (Spivack, 2017). Law enforcement entities have also maintained that the commercial mapping companies provide superior internal analytical tools, the public-facing side is merely a perk and limiting public access to crime data is merely the cost of doing business. In the past, the commercial mapping companies have relied on several legal tools to stop the public from using public crime data on their website.

Copyright

The initial legal strategy to discourage use is copyright, under the claim that the crime mapping companies have transformed the public crime data into a unique, proprietary form, which then provides considerable latitude in controlling the data. In *Georgia v. Public.Resource.Org* (2020), the Supreme Court considered the right of the public to access the Georgia statutory code as provided by LexisNexis. Public Resources is nonprofit dedicated to facilitating access to government information. Public Resources downloaded, then posted online and physically distributed copies of the Official Code of Georgia Annotated (OCGA), which is the state's official statutory code. The OCGA also included annotations produced by LexisNexis, who made intellectual property claims on the additional commentary. The state sued the nonprofit, effectively on behalf of LexisNexis, after a series of cease-and-desist letters went unheeded. The District Court ruled in favor of the state, finding the annotations to be eligible for copyright, while the 11th Circuit reversed, rejecting the copyright assertion under the government edicts doctrine. The Supreme Court affirmed the 11th Circuit's decision, finding the government edicts position compelling and rejecting claims of copyright protection.

While the details of the case are quite similar to those that may hypothetically scrape crime data—government information, third-party copyright claims, LexisNexis's involvement—the case was ultimately decided on narrow authorship technicalities. Also, the government edicts doctrine is unlikely to extend to law enforcement crime data, but the majority opinion also stepped outside of the authorship rationale to observe that there is a right to records and information that aid the public in understanding the operations of government (Georgia, p. 1509). The Court also expressed concern over creating a walled garden for the statutory code with important annotations, while the general public would have the plain language of the code minus necessary context about court cases, amendments, etc. Important distinctions seem to suggest were LexisNexis to make similar copyright claims over crime data pulled from the Community Crime Map, courts would likely find in favor of access. LexisNexis may transform or add value crime data in plotting it, but nearly all parties interested in accessing crime data have no interest in the company's visual display. Individuals seeking crime data merely desire parallel access to the same quality of data, whether that be through government provided access or scraping. The “value” the commercial crime mapping companies add is not what is being sought and thus seems to disqualify copyright claims.

Scraping

Stemming from this ownership claim, the companies rely on broad computer fraud laws meant to deter hacking to discourage the use of scraping. Stripping the functionality (*e.g.*, removing common copy-paste functions) has not deterred more sophisticated users from compiling the data by using a bot or web crawler. And until recently, scraping existed in a gray legal area and

the threat of a lawsuit for violating the federal Computer Fraud and Abuse Act (CFAA) (or other local computer abuse law) was sufficient to discourage some users. However, in *hiQ Labs v. LinkedIn* (2019), the 9th Circuit decided an important case that established scraping to be a legal practice. The CFAA was originally passed in 1986 as an anti-hacking law that sought to punish individuals for unauthorized access to digital properties. The court determined that publicly available data was fair game, even if automated scraping introduced a scale well beyond the capacities of a human. Running automated scripts is not breaking and entering. Then, in 2021, the Supreme Court decided *Van Buren v. United States*, where the Court expanded upon “authorized access.” *Van Buren* vacated *hiQ*, and the case was remanded. On remand, the 9th Circuit redoubled their prior findings. Websites cannot unilaterally enforce limitations in how and why an individual uses their websites. Interestingly, the court adopted a gates up or gates down metaphor in *Van Buren*. Either users are granted access to the information, or they are not. If an individual entered through an open gateway, use of website information is not a crime under the CFAA. *HiQ* and *Van Buren*, collectively, seem to settle the rights of individuals to scrape crime mapping websites.

Terms of use

The crime mapping companies have also filed suit over breach of contract for violating the terms of use individuals agree to when entering the crime mapping website. The companies typically employ expansive terms of use statements to deter use of the crime mapping data. Often called “clickwrap,” as the product cannot be accessed or opened without agreeing to an unavoidable pop-up, these terms can be lengthy, and most website visitors do not have the time or legal acumen to digest their contents. A series of federal cases effectively established that terms of use agreements are legally binding, though there are important considerations, such as affirmative assent, a nondeceptive consent process, and a reasonably prudent person standard. Courts have vacillated though, and more recent rulings have been decided narrowly. At present, there is no categorical ruling, and terms of use agreements are largely determined on a case-by-case basis, but commonplace, nondeceptive terms are generally legal and the terms therein binding.

The mapping companies have varied approaches to terms of use, though they typically error on the side of exhaustive. LexisNexis is likely the most illustrative. In addition to intentionally hobbling third-party use of crime data, the terms explicitly prohibit the use, posting, sale, transmission, distribution, modification, or transfer of the site’s content for public or commercial purposes. There is a provision forbidding the scraping of the data and other language directly disallowing individuals from so much as copying the information. CrimeMapping makes clear that all data and information on the website are the sole property of the law enforcement agency, and that all data is provided voluntarily to the website and use is provisional. However, the website does not transfer any rights of use to the individual. The site also explicitly states that it plays no role in fulfilling FOI requests, and interested parties should work directly with the agency. The CrimeMapping terms are less restrictive than LexisNexis and seem primarily focused on precluding commercial use. The terms also have provisions expressly barring scraping. Motorola’s CityProtect terms explicitly prohibit copying, displaying or other use of the map’s content. The terms of use clearly state that the site and data are solely for personal, non-commercial use. MyNeighborhood site’s terms for use do prohibit reproduction, duplication, copy, sale, etc. of the data, and the terms also discourage scraping a bit more specifically. Generally, the MyNeighborhood terms are much narrower, totaling six brief bullet points rather than the other companies’ pages of legal jargon.

Discussion and conclusion

The recent resolution of mediation involving the Pennsylvania Right to Know Law (RTKL) may prove instructive in considering the future of equal access to crime data (*Suszan v. York*, 2022). Twelve years after abandoning a very similar case in Utah, Reportsee, the small, commercial mapper without access or favor among law enforcement, won a dispute before Pennsylvania's Office of Open Records (OOR). SpotCrime, Reportsee's mapping entity, had routinely requested the same record from the York City Police Department, a month's worth of crime data in an Excel document. The York Police had fulfilled the request without incident for years until July 2022, when they directed SpotCrime to the police blotter and the website of a new third-party crime map operated by Crimewatch Technologies, a small technology company based in York. SpotCrime filed an appeal, arguing their request had inappropriately been denied. SpotCrime said filtering the visual representation on the Crimewatch map was unsatisfactory as it did not allow for downloading or a simple way of copy-pasting the incident report data. The Crimewatch website also had restrictive terms and conditions that severely limited how an individual could use the information. In particular, Crimewatch prohibited commercial use of the crime data. In the formal appeal before the OOR, York stated that directing the requester to the online blotter and the crime map fulfilled RTKL obligations. SpotCrime claimed that to populate a crime map, there had to be existing structured data in some kind of digital table, and SpotCrime sought the file with the digital table whether an Excel file or otherwise.

The OOR, in its binding final determination, decided that the limitations—both the inability to download the data as well as the restrictions on how the data could be used—Crimewatch placed on the crime data meant the records were not fully public and accessible, and thus the RTKL response by the York Police was insufficient. Further, the OOR determined that if York Police could provide Crimewatch with crime data through direct access to their database, then they would need to provide similar access or output the data as requested; a notable victory for access to all databases, as government offices frequently claim the data is not a record (Anderson & Wiley, 2021). However, the narrow technical resolution and the other instances of favoring commercial access to government information still exist. The above legal considerations explore workarounds to accessing crime data—whether terms of use are enforceable, whether scraping is legal, and whether claims of ownership are legally plausible in deterring the public from using crime data—but structural solutions are needed. A more direct route would not rely on circumvention and instead address the principles of whether and why the public should be granted equitable access to crime data.

There are several solutions that would curb the practice of discriminatory distribution of crime data. The simplest solution would explicitly make crime data a public record subject to FOI laws or affirmative disclosure. There would be no evasiveness if the confusion regarding the public's right to the data was eliminated. Given the discourse, resources and current scrutiny of law enforcement, an access to crime data provision would seem to be sensible and palatable legislation. Another possible solution is establishing parallel access: a legal principle that requires any government information transferred to a commercial entity also be made available to the general public. Information could be made subject to conventional FOI exemptions or other existing restrictions to release. The locus for distribution can be on the government or the company, but the quality, frequency, and format of the data must be identical. Adoption of parallel access

presents the potential for a dramatic expansion of the amount of government information circulated and ensures information equity across government.

The most aspirational of the solutions is recognizing a generalized right of access to government information. Scholars have found a constitutional right of access to be elusive (BeVier, 1980; Cooper, 1986; Jordan, 2004), but a constitutional right to know could provide a substantive impact, ranging from a kind of benefit of doubt in court rooms to catalyzing a sea change in how access and transparency are conceived and realized. Any generalized right of access would be dependent on the boldness of the language, and it must be noted Florida, a state with a constitutional right of access, has similar access and crime data issues as states without. It can signal a dramatic change in a country, state, or jurisdiction's commitment to transparency, but the manifestation of meaningful change is in the follow-through and the many small decisions of dispersed records custodians and local judges. While ambitious, the concept is not new and has deep roots in right to information movements abroad. Many foreign constitutions include provisions guaranteeing citizens access to government information. Multinational collectives, like the United Nations, have recognized a right to receive information as a universal human right. The instance of crime data seems tailor made as the type of case where a right of access might tip the scales.

Crime maps are not the problem. The favoritism shown to commercial mapping companies is, however. Crime maps are likely viewed by most localities as a welcome perk; a free service on top of their necessary public safety administration systems, and any restrictions on sharing the crime data are the cost of providing the public with crime maps. But there is simply no justification for granting a commercial entity preferred or exclusive access. It is contrary to fundamental democratic principles, and the practice overtly circumvents FOI laws. Allowing commercial entities to dictate the terms of access to crime data is not equal access. The practice is especially galling as access to incident-level crime data has value to other parties, be they civic-minded individuals, scholars, or other commercial entities. Court records, state codes, local regulation, and building codes have all experienced similar ownership and access issues. It has proved quietly intransigent as well with the practice being observed for more than a decade. Public-private partnerships, particularly in regard to technology and data practices, are common and growing. It is past time to address this inequity in access to government information.

References

- Asher, J. (2022). The FBI's next set of crime data is going to be a big mess. *The Atlantic*. <https://www.theatlantic.com/ideas/archive/2022/05/fbi-crime-data-nibrs-2021/629797/>
- Anderson, J., & Wiley, S. K. (2021). Freedom of the database: Auditing access to structured data. *Journal of Civic Information*, 3(1), 3-56.
- BeVier, L. R. (1980). An informed public, an informing press: The search for a constitutional principle. *California Law Review*, 68(3), 482-517.
- Chainey S., & Tompson L. (2012). Engagement, empowerment and transparency: Publishing crime statistics using online crime mapping. *Policing; A Journal of Policy and Practice*, 6(3), 228-239.
- Cook, S. J., & Fortunato, D. (2022). The politics of police data: State legislative capacity and the transparency of state and substate agencies. *American Political Science Review*, 1-16.
- Cooper, P. J. (1986). The Supreme Court, the First Amendment, and freedom of information. *Public Administration Review*, 46(6), 622-628.
- Cuillier, D. (2010). Honey v. vinegar: Testing compliance-gaining theories in the context of freedom of information laws. *Communication Law and Policy*, 15(3), 203-229.
- Delaney, C. (2020). Police transparency solution released. *ArcGIS Blog*. Retrieved from <https://www.esri.com/arcgis-blog/products/arcgis-solutions/public-safety/police-transparency-solution-released/>
- Doty, P. (2000). Freedom of information in the United States: Historical foundations and current trends. Retrieved from https://moody.utexas.edu/sites/default/files/foia_doty_2000.pdf
- Fenster, M. (2017). *The transparency fix: Secrets, leaks, and uncontrollable government information*. Stanford, CA: Stanford University Press.
- Georgia v. Public.Resources.Org. (2020). 140 S. Ct. 1498.
- Groff, E. R., Kearley, B., Fogg, H., Beatty, P., Couture, H., & Wartell, J., (2005). A randomized experimental study of sharing crime data with citizens: Do maps produce more fear? *Journal of Experimental Criminology* 1(1): 87-115.
- HiQ Labs v. LinkedIn (2019). 938 F.3d 985, 9th Circuit Court.
- Hochberg, A. (2013). Disputes over crime maps highlight challenge of outsourcing public data, *Poynter*. <https://www.poynter.org/reporting-editing/2013/disputes-over-crime-maps-highlight-challenge-of-outsourcing-public-data/#.UZ5vqZK8Ulc.blogger>
- Ingrams, A. (2017). The legal-normative conditions of police transparency: A configurational approach to open data adoption using qualitative comparative analysis. *Public Administration*, 95(2), 527-545.
- Jordan, A. (2004). The right of access: Is there a better fit than the First Amendment. *Vanderbilt Law Review*, 57(4), 1,349-1.386.
- Kimball, M. B. (2003). Law enforcement records custodians' decision-making behaviors in response to Florida's public records law. *Communication Law and Policy*, 8(3), 313-360.
- Li, W. (2022). What can FBI data say about crime in 2021? It's too unreliable to tell. *The Marshall Project*. https://www.themarshallproject.org/2022/06/14/what-did-fbi-data-say-about-crime-in-2021-it-s-too-unreliable-to-tell?utm_medium=email&utm_campaign=newsletter&utm_source=opening-statement&utm_term=newsletter-20220614-2872
- NARA v. Favish (2004). 541 U.S. 157.
- NLRB v. Sears, Roebuck, & Co. (1975). 421 U.S. 132.

- NLRB v. Robbins Tire & Rubber Co. (1978). 437 U.S. 214.
- Palmer, G. (1998). The new spectacle of crime. *Information, Communication & Society*, 1(4), 361-381.
- Pozen, D. E. (2016). Freedom of information beyond the Freedom of Information Act. *University of Pennsylvania Law Review*, 165(5) 1,097-1,158.
- Quinton, P. (2011). The impact of information about crime and policing on public perceptions: The results of a randomized controlled trial. *National Policing Improvement Agency*.
- Scassa, T. (2016). Police service crime mapping as civic technology: A critical assessment. *International Journal of E-Planning Research*, 5(3), 13-26.
- Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society*, 18(4), 581-599.
- Spivack, M. (2017). How private contractors are taking over data in the public domain, *Reveal*. <https://revealnews.org/article/how-private-contractors-are-taking-over-data-in-the-public-domain/>
- Suzan v. York (2022). OOR Dkt. No. AP 2022-1894.
- U.S. Const. art. I, § 5.
- Van Buren v. United States (2021). 141 S.Ct. 1648.
- Vera Project (2022). Police data transparency index. <https://www.vera.org/research/police-transparency-index>
- Wagner, A. (2021a). Pandering, priority or political weapon: Presidencies, political parties & the Freedom of Information Act. *Communication Law and Policy*, 26(1), 387-426.
- Wagner, A. (2021b). Piercing the veil: Examining demographic and political variables in state FOI law administration. *Government Information Quarterly*, 38(1), 1-10.
- Wallace, A. (2009). Mapping city crime and the new aesthetic of danger. *Journal of Visual Culture*, 8(1), 5-24.
- Westrope, A. (2019). Motorola parts with Socrata, ends access to open crime APIs. *Government Technology*. <https://www.govtech.com/biz/motorola-parts-with-socrata-ends-access-to-open-crime-apis.html>
- Wilson, J. Q. (2002). Crime and public policy. In (James Q. Wilson. & Joan Petersilia, eds.) *Crime: Public Policies for Crime Control*. Oakland, CA: ICS Press.
- Wisnieski, A. (2014). Is your city's crime data private property? *Recode*. <https://www.vox.com/2014/5/5/11626460/is-your-citys-crime-data-private-property>