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). Public Engines’s lawsuit included claims that Reportsee had committed computer fraud, breach of contract, hot news misappropriation and violated the Lanham Act and the Utah Anti-Cyberterrorism Act.

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 around the country. 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 publish this information online, including plotting the crime data to their public website, CrimeReports. Reportsee mapped similar crime data but without the proprietary software or preferred access. Reportsee was more opportunistic in seeking crime data, typically asking for a feed from law enforcement agencies while also relying on varied other trustworthy sources. 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 their competitor’s website, because law enforcement entities across the country 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 public records 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 may be arguments that the information may not meet the statutory definition of a record in some jurisdictions, but if a government entity is distributing it to one party, then it would be odd to refuse to distribute it 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, in geographies across the country, receiving preferred or exclusive access to crime data, and sometimes even claiming ownership of the data.

Since the lawsuit was settled, there has been little news or direct legal action, but 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 compilation and maintenance 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. Digitization of government records has added access in many ways, but it has also proved to be yet another hinderance in establishing government transparency. Beyond the principle of equitable access, there are legitimate concerns about the social effects of crime mapping. There is anxiety over what these maps accomplish, particularly concerns over perpetuating surveillance culture that rests on dubious law enforcement practices and contributing to cognitive biases that leave the public with exaggerated sense of danger in their communities.

In surveying the status of crime maps in the United States, the manuscript found crime mapping to be common among law enforcement websites. The study found 65% of the 250 largest U.S. cities’ police departments host a crime map on their website, and the manuscript proposes a reevaluation of the practice as a whole. First, the manuscript surveys the present status of crime data in the United States, followed by review of literature on crime mapping and government data issues. The manuscript then considers the implications of crime mapping. Then the manuscript surveys 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 an end to preferred commercial access and proposes solutions to the problem.

**The Status of 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 little more than old aggregate crime statistics, while many offer 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.

To complicate matters, the FBI 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 has severely weakened crime data across the country. 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 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 is 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 and determined the general state of crime data to be very poor. In evaluating 10 categories of data transparency, the highest scoring city, Chicago, earned a 70 (out of 100) and only 21 of the 94 scored higher than 50 (Vera Project, 2022).

Beyond the fundamental counting and publishing of information on crime, there exist many concerns about the state of crime reporting in the United States, and many of these
concerns are tied to the commercial implications in adopting technology. Law enforcement agencies have built commercial relationships in growing the public-private surveillance network, including commonly distributing Ring cameras at no cost to citizens. Skeptics fears were confirmed when Amazon admitted to providing law enforcement with Ring video without user consent (Belanger, 2022). Another uneasy law enforcement relationship involves promoting the neighborhood social media platform Nextdoor, which sells itself to police as a crime monitoring tool. The company explicitly seeks to align itself with public institutions. Law enforcement websites often include links to local Nextdoor pages, and the company produces a law-enforcement-facing app specifically for use in monitoring citizens.

Ring and Nextdoor are both part of a growing trend where tech companies foster strong relationships with law enforcement, and increased reliance on third-parties technology allows for increased surveillance presence while avoiding accountability. 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 (Wisnieski, 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.

**Literature review**

**Crime Mapping**
Scassa (2016) defined geolocated crime data: “Publicly accessible crime maps offer 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 crimes 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) suggested crime maps also produce some academic value and meet a self-evident public interest in crime and its whereabouts.

Scholars have been critical though of what the maps accomplish and long on the consequences of these efforts. Wallace (2009) offered a broad critique of the practice. She argued publishing of crime statistics is an advertisement for the effectiveness of law enforcement, both justifying their work and acting as 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 solution and reach the right conclusions in a timely manner” (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. Her largest concern stemmed from the disembodying of real-world problems. She claimed crime maps contribute, like traditional news media, to a view of crime as simple and straight-forward problem, instead of a complex social issue.

Chainey and Thomson (2012) surveyed crime mapping in the United Kingdom, which mandated nation-wide 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. And they searched for 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). Interestingly, they found a huge initial interest in the crime maps, followed by a sharp decrease in online visitors to the pages. Ultimately, 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 (2016) 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 CrimeReport, since bought and shuttered by Motorola. Scassa, like her predecessors, was ultimately fairly pessimistic about the impact of crime maps. She suggested they are of limited use and likely not as valuable as they may appear at first glance. 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 an especially cogent point about 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. Furthering this, 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. Despite good intentions, the crime maps contribute to urban crime narratives and succumb to top-down, technology-driven ideals of civic engagement without the promised benefits.

More Data, FOI Laws & Digital Transparency

Important other considerations include conflating crime mapping efforts with thorough-going accountability measures; or, as Chainey & Tompson called it, confusing theater of transparency for meaningful accountability. Open government efforts, like crime mapping, are ideologically akin to bedrock transparency laws, like freedom of information (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 government information. More information from the government should generally be applauded, but it should not be confused with or accepted as a substitute for real transparency measures, despite the stated objectives of the crime mapping companies.
Technology, in many ways, has improved government transparency, but too often digital advances become another dodge for transparency and accountability. Originally crafted in an era of hard-copies, FOI laws have struggled to keep apace of new digital records formats, as well as digital transfer and storage (McCammon, 2022). The advent of encrypted messaging apps, along with basic text messaging and the (often illegal) use of private email, have proved highly problematic to public records requesters (Stewart, 2019; Wagner, 2019).

Meijer (2018) coined the term “datapolis” in observing the transition to more technology-reliant cities, suggesting that the future of smart cities is persistently presented as both inevitable and beneficial. The presumption is that technology delivers safer, wealthier and greener cities. Often, discussion of new civic technologies elides the inherent political and value-laden choices in implementing new technologies. Wallace agreed, encouraging the public to remain cognizant that technology choices are predicated on systems of value, not necessarily facts. Meijer noted data visualization and data access as two of the principal challenges of the modern smart city. More digital technology creates more data and more possibilities for accountability, but in these new instances, the possibility for transparency must be weighed and ultimately forged anew. Transmitting hourly crime data to the public was inconceivable three decades ago. Now, it is not only possible but relatively simple to do so in an attractive visual display. But the public must consider the political and social implications of this choice. And as Usher (2020) observed, the ubiquity of data and, in particular, mapped data will only grow, and the public must confront the importance of place and the representation of place. Meijer warned of government-commercial partnerships, suggesting these shape data collection, custodianship and distribution. He foregrounded data storage with a special interest in ownership of data. Ownership is central to all successive characteristics or uses of data. When governments agree to either sell civic data or
provide particular rights as part of a legal agreement, the civic benefit of the data can be destroyed. Meijer concluded that the datapolis is not inherently bad or something to be feared, but something to be created with an awareness of the threats that accompany techno-utopianism. It is not hard to see crime mapping as a fairly clear reification of Meijer’s conception of a smart city, nor hard to notice some of his warnings being manifested.

**Cultivation Theory and Mean World Syndrome**

While some of Meijer’s more concrete concerns about the proliferation of civic data have materialized, there are other less readily visible issues to consider. Gerbner’s (1969) cultivation theory, which proposed that an individual’s media consumption affects their perception of reality, is relatively simple on its surface. But cultivation theory is important in making the distinction that media consumption may not drive outward behavior but has a profound impact on how an individual views the world. Gerbner’s theory was pivotal in establishing that exposure to violence did not produce a violent viewer but instead a creeping increase in fear and mistrust.

He analyzed television consumption to determine whether and how it affected attitudes and perceptions of the world, finding that the opinions of those that consumed more television more closely aligned with the messages of the television programming. Most notably, research showed that heavy exposure to violent television produced an exaggerated perception of crime and higher levels of fear (Gerbner et al., 1979; 1980). Gerbner et al. (1980) and others, namely Signorielli (1990), coined and confirmed the existence of “mean world syndrome,” where long-term exposure to television cultivates a perception of a mean and dangerous world. Given the contemporary information environment, too much should not be made of a theory founded on the number of hours of television consumption. It is undoubtedly a very different atmosphere for
news intake, but the underlying sentiment of mean world syndrome—perceptions can become unmoored from reality with too much exposure to fear-inducing content—seems somewhat durable, and scholars have found mean world syndrome in exposure to contemporary media. There is evidence that non-fiction media exposure generates fear in the public (Chiricos, Escholz & Gertz, 1997). Police reality shows, such as “Cops,” were also found to produce fear (Holbert, Shah & Kwak, 2004). Scholars have also found local television news with more reportage on crime predicted increased fear and higher perceptions of crime (Romer, Jamieson & Aday, 2003). While crime maps represent a facsimile of reality, they inflame concerns and ultimately represent another source of crime information in an information environment already saturated in crime, and this ongoing conversation has deleterious psychological and social effects.

The commercial crime mapping companies advertise their products to law enforcement on the promise of stronger data analytics and the ability to adapt policing practices according to the enhanced analysis. These analytics-based evolutions in policing practices present a disconcerting future, including the possibility of predictive policing, which mapping companies have explicitly advertised (Andrejevic, Dencik & Trere, 2020; Wallace). It bears noting that crime mapping ties together the negative attributes of street-level imagery with the broken windows theory of law enforcement (Shapiro, 2018). Broken windows is a discredited policing practice that focuses police attention on problem areas under the belief that a broken window or other sign of crime or disorder naturally precedes more crime. Not surprisingly, the theory increased aggressive policing, attention was disproportionately focused on minority neighborhoods and ultimately increased social inequity (Harcourt, 2001; Harcourt & Ludwig, 2006; Legewie & Fagan, 2019). Law enforcement must review policing and crime activity
through data analysis, but under no circumstances should agencies adopt predictive policing or rely on software whose analysis relies on a debunked and racist premise.

**Crime Mapping Companies**

Crime maps are currently quite popular. The author reviewed the general city and police websites of the 250 cities in the United States with the largest populations, and 65% hosted or linked to a map with crime information. The survey found five crime maps: LexisNexis’s Community Crime Map, CentralSquare Technologies’s CrimeMapping, Motorola’s CityProtect, Corona Solutions’s MyNeighborhood and in-house.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Crime Maps in U.S. Cities with Largest Populations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product (Company)</td>
<td>n</td>
</tr>
<tr>
<td>Community Crime Map (Lexis Nexis)</td>
<td>61</td>
</tr>
<tr>
<td>CrimeMapping (CentralSquare)</td>
<td>45</td>
</tr>
<tr>
<td>CityProtect (Motorola)</td>
<td>9</td>
</tr>
<tr>
<td>MyNeighborhood (Corona Solutions)</td>
<td>4</td>
</tr>
<tr>
<td>In-house</td>
<td>46</td>
</tr>
<tr>
<td>No map</td>
<td>87</td>
</tr>
<tr>
<td>Total</td>
<td>252</td>
</tr>
</tbody>
</table>

Note: Two cities had two crime maps.

The four commercial options come with restrictions, while the in-house version represents a map that is produced by member of the city’s payroll, often a citywide mapping or GIS department. In rare instances, law enforcement offices had their own mapping team.
Commercial

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.
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 usability 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.

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 that 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 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 cities, produced their own in-house map. And this seems like a product of the Obama-era federal push for cities to produce more data, including mapping shapes and layers. As a result, many U.S. cities developed open data portals that house a wide range of city data. 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 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 seems to encourage the sharing and reproduction of noncommercial content.

**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 the law enforcement agency refers the individual to the map or 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 some 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). 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 websites. 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. Stemming from this ownership claim, the companies rely on broad computer fraud laws meant to deter hacking to discourage the use of scraping. 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. These terms typically include a comprehensive claim on any and all use of the crime data. There is not a great deal of legal discussion on the specific matter of access to crime data, but there are recent federal cases that undercut the companies’ legal efforts to control crime data.

Terms of Use

Commercial mapping companies employ expansive terms of use statements to deter use of the crime mapping data. It is blunt tool, and federal courts have considered the ubiquitous terms of service agreements. 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 aughts-era federal cases effectively established that terms of use agreements can be legally binding, though there are important considerations, like affirmative assent, the presence of a nondeceptive consent process and a reasonably prudent person standard. Courts have vacillated though, and more recent rulings have been ruled 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 scrapping. 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.

In addition to the obligatory terms a website visitor accepts, there are also the contracts the law enforcement agencies enter into with the commercial companies to consider. The standard contract cities and their law enforcement agencies sign when providing their crime data to LexisNexis begins a relationship where the city joins a LexisNexis-maintained public safety data exchange where all active law enforcement agencies post and share crime data. The city and the law enforcement agency, per the contract, “at no charge, hereby grants to LN a paid up, irrevocable, worldwide, non-exclusive license to use, adapt, compile, aggregate, create derivative works, transfer, transmit, publish and distribute” the city’s crime data contributions. The
customer retains ownership of the data, but any and all representations of the data on the Community Crime Map are under the sole ownership of LexisNexis. In reviewing the contracts cities enter into when joining CrimeView, the underlying data base for CrimeMapping, under ownership and rights, clients contributing to the database grant CentralSquare/TriTech the right, without limitation, to use any data and information that is uploaded, inputted or otherwise submitted.

**Scraping**

To maintain control of the crime data, commercial mapping companies have taken legal action to stop scraping of their websites. 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, it is not a crime under the CFAA. *HiQ* and *Van Buren*, collectively, seem to settle the rights of individuals to scrape crime mapping websites.

**Copyright**

In *Georgia v. Public.Resources.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, 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.

Together, the recent federal decisions point toward public access to crime data, even if by scraping, which is effectively an end-run. To be fair, the companies do not seem especially dedicated to stopping such efforts. While they do strip functionality and place unnecessary restrictions on the crime data, some companies do offer the data in tabulated form. They may not be entirely hostile to the practice, but the principle remains. Commercial companies should not get exclusive or preferential access to public crime data.

Conclusion

The manuscript presents a narrow access issue, but the issue of crime data also presents another example of the difficulty in acquiring information from the government and another demonstration of the particularly challenging nature of accessing information held by law enforcement, an institution notorious in the requesting community for its truculence in abiding
by FOI laws and general resistance to transparency. 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.

Crime mapping, writ large, must be reevaluated. The companies advertise increased civic engagement and more transparency, but there is no evidence to suggest either of these occur. Any civic engagement is thin and of a voyeuristic nature, while any claims of transparency to be hollow and insufficient in manifesting real accountability. The costs of crime mapping must be seriously weighed against the unsubstantiated claims of benefit. Beyond the first-order question of whether crime maps are constructive social tools is the disconcerting practice of providing commercial entities exclusive or preferred access to government information. 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. 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, and they range from targeted statutory provisions explicitly banning the practice to establishing a generalized right of access to all government-held information. The simplest solution is to simply bar transfer of crime data to commercial entities. There would likely be undesired consequences to this, but it would ensure corporations are not placed ahead of the public. Another dire t solutions 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 ensure information equity across government.

The most aspirational of the solutions is recognizing a generalized right of access to government information. 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 would also be at the discretion of judges to substantiate. 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 roots both in international right to information efforts. 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. The right to access to crime data is liminal and requires reading between the lines. At present, law enforcement entities often resist releasing
crime data through various dubious legal claims, but language that prioritizes access to
government information can cut through such ambiguity.

Technology has produced many new affordances and required many reckonings. Meijer
observed that technology is neither inevitable nor certain to be beneficial. Nor are technologies
intractable, and it is time to reconsider crime maps and not merely accept them on
unsubstantiated promises. Crime maps are likely viewed by most localities as welcome
lagniappe; a free service on top of their necessary public safety administration systems. But it is
fairly clear these crime maps serve little meaningful public good and also come with significant
harms—most notably in perpetuating criminal stereotypes founded on questionable law
enforcement practices and boxing out public access in favor of commercial enterprise—and it is
time to reconsider the experiment with crime maps. Whether the practice of crime mapping
needs to stop wholesale is worth considering, but handicapping public access in favor of
commercial entities requires little further rumination. There is no justification for doing so, and it
only compounds the harms of an already questionable practice.
References


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*, 22 May. Available at: https://www.poynter.org/reporting-editing/2013/disputes-over-


