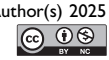
Normal manuscript

Digital punishment, lateral surveillance & the sex offense registry

Punishment & Society
1–23


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14624745251370758
journals.sagepub.com/home/pun


Sarah Lageson[1] and Chloé Sudduth[2]

Abstract

The maintenance of a public sex offense registry has been codified as a non-punitive civil policy since the 2003 Supreme Court case of *Smith v. Doe*. But since then, sex offense registries have transformed from a centralized state repository of information to a sprawling digital archive of personal data about people required to register. We identify and report the current technological capabilities of state-run sex offense registries through a 50-state survey and draw from the analysis to argue that the digital turn has changed the form and function of the registry. While the Court saw registries as analogous to a trip to an archive, our data show how registries now exert digital punishment and lateral surveillance through state-enabled technical capabilities on registry websites. In a departure from earlier schemes that required users to conduct a targeted search on a government-run website, registrants' personal information is now routinely harvested and posted for profit motives in the private sector. Such shifts require a new analysis of sex offense registries; one that specifically interrogates at what point technology transforms a civil, purportedly non-punitive public policy into a decidedly punitive measure.

Keywords

technology, surveillance, punishment, sex offense registries

[1]Northeastern University, USA
[2]Rutgers University-Newark, USA

Corresponding author:
Sarah Lageson, 401F Churchill Hall, 360 Huntington Ave, Boston, MA 02115, USA.
Email: s.lageson@northeastern.edu

Introduction

The advent of public sex offense registries signaled a new approach to those already subjected to criminal punishment. For people convicted of a qualifying sexual offense, inclusion on the registry means any member of the public could learn about their conviction through a centralized state repository. While registries created new avenues for public stigmatization, legal challenges led the nation's highest court to deem that, rather than expressly punishing, registries are a legitimate, civil, nonpunitive measure (*Smith v. Doe* 2003, 538 U.S. 84 (2003)).

Yet, the technological landscape has shifted dramatically since the *Smith* decision. In November 2002, the month *Smith* was argued, only 15% of Americans had broadband internet access in their homes. Today, 96% of the public routinely uses the internet (Pew, 2024). Beyond access, technological capabilities have dramatically changed the form, function, and reach of registry information. Third party software platforms running on state websites allow for the active tracking, mapping, and direct notification of registrants' status updates, home addresses, and work locations. Some state registries allow registry data to be instantly exported into a bulk data file with a single click. Data about registrants are scraped and aggregated by private third-party data vendors, contributing to the spread of such information in private data repositories and websites that are unregulated by the state. In a departure from the earlier schemes that required users to conduct a targeted search for particular registrants on a government-run website – and indeed, the type of registry in front of the Supreme Court in 2003 – registrants' personal information is now routinely harvested and shared. These changes in how the internet organizes and disseminates registry data means that registrants' personal information is routinely disseminated to internet users who are not even looking for such information. State website design choices, such as creating browsable registries and instant methods to share registrant information with friends and send tips to the state, create additional opportunities for lateral surveillance and surveillance deputization. Vigilante groups on loosely regulated social media platforms then use these data to harass and stigmatize those who are registered, leading to both virtual and in person harms.

Such shifts require a new analysis of sex offense registries; one that specifically interrogates at what point technological changes transform a purportedly civil, non-punitive public policy into a decidedly punitive measure. Through a 50-state survey, our analysis details the technological capabilities and punishment implications of the digital sex offense registry of today. We frame our analysis within the broader punishment and society landscape, linking our study to recent punishment and society work that has highlighted how legal system actors and the broader public characterize people convicted of sex offenses as irredeemable and dangerous (Janus 2006; Lynch, 2002; 58-59; Werth, 2023), and when coping with stringent civil restrictions, sweep those around them into the surveillance apparatus of registration (Leon and Kilmer, 2023). As we argue, the digital architecture, design choices, and technological capabilities of today's registries further cement the notion of a risky and dangerous subject that requires constant digital surveillance across public and private sector databases. While our analysis raises legal policy questions regarding the relevance of the *Smith* decision in today's

technological landscape, we also invoke broader sociological questions about the role of the sex offense registry in our contemporary understandings of how punishment is deployed in the digital domain.

Background

The advent of sex offense registries

People convicted of a sex offense have long been viewed by the public and the criminal legal system as "especially aberrant, predatory and irredeemable" (Werth, 2023: 977). Criminalization efforts have centered on protecting children (Meiners, 2016) and the widespread belief that people convicted of sexual offenses are "a very sick group" (Spencer and Ricciardelli, 2017) of "monsters beyond repair or redemption" (Werth, 2023: 978). Responsive policymaking has expanded to encompass what scholars have deemed a "new punitiveness" (Pratt, 2000), marked by the mandated registration of people into publicly accessible databases. Policy choices to publicize, often for life, this specific set of offenses is often rooted in beliefs that individuals convicted of sexual offenses are a unique group with particular pathologies that render them more likely to commit future sexual harm. However, rates of sexual reoffending are quite low (Przybylski, 2015), even though recidivism rates among people convicted of sexual offenses are notoriously difficult to measure and are varied across study contexts (Lussier et al., 2024). Some studies also point to violations as more likely to emerge from compliance with registration requirements rather than new sexual offenses (Tewksbury et al., 2012). Empirical research on sex offense registries suggests that they do very little to prevent sexual crime (Agan and Prescott, 2021). Even amidst this evidence, publicly accessible digital registries remain available in every state and at the federal level.

But while sex offense registries seem ubiquitous today, they are a relatively recent approach, beginning with the 1994 Jacob Wetterling Act that established initial registration standards and created the "Sexually Violent Predators" classification. This was followed by Megan's Law in 1996, which mandated public disclosure of registrant information, and the Pam Lychner Act, which established the first national database for law enforcement. Throughout the late 1990s and early 2000s, legislation continually expanded registry requirements, communication infrastructure between agencies, and public accessibility of information. The 2006 Adam Walsh Child Protection and Safety Act marked a significant development, creating the three-tier classification system, establishing the SMART Office within the Department of Justice, and implementing the Sex Offender Registration and Notification Act (SORNA), which made failure to register a federal crime.

Registries soon became available as searchable websites run by state governments. Legal challenges followed, culminating in the U.S. Supreme Court Case *Smith v. Doe* (2003), in which two Alaskan residents who were required to retroactively register for an offense that pre-dated the registry challenged the constitutionality of the state policy under the Ex Post Facto Clause of the United States Constitution. The 9th Circuit held that, because it was punitive *in effect,* regardless of its intention, the policy violated

the Ex Post Facto Clause. Yet, in a 6-3 decision, the Supreme Court held that the Act was non-punitive and, therefore, did not violate the Constitution. The Court reasoned that the Alaska policy was intended as a civil process to identify those convicted of sexually oriented offenses for the awareness and protection of the public. The Court also found that any stigma that may result was non-punitive because it did not impose any physical restraint or affirmative disability.

In subsequent challenges to registries, courts continue to rely on a test to determine whether registries constitute punishment that first analyzes legislative intent to punish. If such intent is found lacking in the statute authorizing the registry, the court then looks at whether "the law is nonetheless so punitive either in purpose or effect as to negate the State's nonpunitive intent" (*Doe v Miller*, 405 F.3d 700, 718 n.6 (8th Cir. 2005)). This analysis asks whether the policy or practice in question has "been regarded in our history and traditions as punishment; imposes an affirmative disability or restraint; promotes the traditional aims of punishment; has a rational connection to a nonpunitive purpose; or is excessive with respect to this purpose" (*Smith* at 97). These factors derive from case law established in *Kennedy v. Mendoza-Martinez* (372 U.S. 144, 168–169) and require courts to seek clear proof that a civil remedy has transformed into a criminal penalty in its effect (*Smith* at 92).

To date, legal challenges to registries based on this analysis have largely failed. And while the Supreme Court created legal precedent regarding the purportedly non-punitive nature of registries, empirical and theoretical research has long questioned the Court's logic in *Smith*. Accordingly, our study asks a broader sociological question of whether and how the technological capabilities of today's registry should alter this legal test; specifically, whether the "digital punishment" (Lageson, 2020) of the registry changes the calculus.

Legal exclusions

People on the registry must contend with statutory registration requirements and legal exclusions regarding residency and employment sectors, alongside heightened collateral consequences for the underlying conviction. All states require registrants to report their full name, any aliases, date of birth, residential address, phone numbers, social security number, travel documents, employer name and address, school name and address, professional licenses, vehicle information, physical description, offense information, criminal record history, driver's license or identification card, a DNA sample, fingerprints, and a current photograph (n.d.; Reed, 2017, US DOJ 2021). While some of this information is not available on public SORNA websites, much of the rest can be publicly accessed at any time by anyone with access to the internet.

Registrants must share this information with the state for the duration of their registration requirement. Many states classify individuals convicted of sexual offenses by Tier I, II, or III based on their offense. Tier I registrants typically have a minimum registration period of 15 years. Tier II has a minimum of 25 years and Tier III has a lifetime registration requirement. Jurisdictions also have discretion to push registration requirements beyond these minimums, with some choosing to avoid the tiered classification system altogether and subject all individuals convicted of sexual offenses to lifetime registration

requirements (Reed, 2017). Failure to update the state when there is a change in any required registration information, for instance, when moving, can result in being charged with failure to register. Individuals who knowingly fail to register or update their information can serve up to ten years in prison (Reed, 2017).

Registration impacts housing, employment, and social life. Registrants are often subjected to residency restrictions (Byrne et al., 2022; Leon et al., 2023; Williams, 2018) near schools, daycares, playgrounds, recreation centers, parks, and sometimes movie theaters, sports facilities, amusement parks, and libraries (Meloy et al., 2008). Local jurisdictions can add additional restrictions amounting to a banishment of those subject to registration (Levenson, 2008; Reed, 2017; Tewksbury, 2007; Yung, 2007). These residency restrictions are often described as an effort to keep registrants away from children to prevent potential victimization and enhance public safety, but several studies have found that residency restrictions do not lower sexual recidivism rates (Nobles et al., 2012; Walker, 2007; Wright, 2014). Instead, these restrictions make finding housing challenging and push many registrants into more rural areas and into homelessness (Meloy et al., 2008). Relatedly, many states will not allow individuals who are required to register to work at childcare facilities, schools, recreation centers, and other places in which children spend time, contributing to higher rates of unemployment for registrants (Tewksbury and Zgoba, 2009). These restrictions create what punishment scholars describe as a class of "secondary registrants," where legal and extralegal surveillance is extended to the family members of registrants (Leon and Kilmer, 2023).

Not only are registrants subject to the SORNA websites that publicly post their information, but their ability to interact on the internet is often limited by law as well. Individuals can be required to report email addresses and internet identifiers, such as social media handles and screen names, for monitoring by law enforcement (Reed, 2017). Specific social media sites may be banned, or in some cases, individuals are banned from using the internet entirely (Regina, 2012; Tewksbury and Zgoba, 2009). Several states allow or provide for surgical and chemical castration as a sentencing factor (Cooper, 2025; Norman-Eady, 2006). These extreme and enduring collateral consequences are beyond the scope of what is faced by others involved in the legal system and are often buttressed by pervasive public fear of people convicted of sexual offenses (Kernsmith et al., 2009).

The collateral harms of registration are also deployed by non-state entities. Researchers have long documented stalking, threats, harassment, and violence against registrants (Tewksbury, 2005). Today, digital vigilante watchdogging fundamentally contributes to punishment beyond the state and has included physical violence perpetrated against registrants that is filmed and streamed on social media as content known as "pedophile hunting" (Toler and Bedi, 2025). The hashtag #shootyourlocalpedophile on Twitter and TikTok reveals substantial social media activity around using public registry information to identify, shame, and threaten real life harm to registrants (Kozlowska, 2019; Purshouse, 2020). The digital nature of today's registries alongside a persistent moral panic about those convicted of sexually oriented offenses has manifested in a form of "violence entrepreneurship" that profits from a sensationalized public display of punishment and shaming (Toler and Bedi, 2025).

Punishment, surveillance & the registry

Today's public registry may be best understood through theoretical concepts of expressive punishment, risk management, and penal entrepreneurialism—regardless of the Supreme Court's "civil" designation. Punishment scholars have long analyzed the expressive functions of policy responses to crime (Garland, 2018), often rooted in Durkheim's (1900/1973) foundational views of the moral and cohesive role of punishment in society and the broader structure and function of penal systems (Foucault, 1977; Melossi and Pavarini, 1981). This scholarship describes punishment as a socio-political practice that carries functions beyond retribution for wrongdoing, leading to mass punishment (Campbell and Schoenfeld, 2013; Cohen, 1985; Goodman et al., 2017) and often rooted in risk governance (Feeley and Simon, 1992; Simon, 2007). The registry is thus emblematic of what Garland (2018) characterizes as a specific type of penal phenomena "not to be understood as a simple reaction or response to crime," but rather as a force that has its "own dynamics and determinations"—a form of control that is "selected for symbolic rather than instrumental effect" (Garland, 2018: 16). Registries are not only designed to prevent future crime, but rather to serve the instrumental purpose of indicating moral boundaries, reifying state authority, managing societal anxieties and governing risk through managerial techniques (Feeley and Simon, 1992). As risk narratives emerge, there is an effort to quantify, assess, and know the risks to ward off potential danger (Garland, 2001). The state, in part, constructs and renders legible the risk posed by the dangerous sex offender that must be managed. The registry, particularly in the digital context, becomes a tool for social control that is directly shaped by expressive, social, and cultural dynamics, rather than a utilitarian means to an end.

Punishment and society literature has long noted how the state frames people convicted of sex crimes as "authentically violent" "monsters" who intentionally harm others (23-61). This specter of dangerousness has animated the growth and maintenance of the public registry. The legal construction of sexually violent predators, alongside the use of actuarial risk assessments in civil commitment proceedings and the deployment of forensic psychology, creates a "distinct type of person requiring exceptional penal measures" (Vogler, 2018: 510). Such exceptional measures include intensive surveillance and "severely curtailed liberties" through lifetime legal requirements that "promulgate the idea that sex offenders are incurable deviants" (Vogler, 2018: 519). As the concern about the risk posed to society by those convicted of a sexual offense grew, the state needed to improve (or appear to improve) their risk management and prevention measures. The actuarial approach to managing the risk posed by "sexually violent predators" became rooted in a socio-technical approach to track, surveil, and publicly label—which has evolved with technological advancements of geolocation mapping, notification systems, and searchable public databases. These capabilities expand the original purported intention of the registry and are framed as both efficient and effective at risk management.

Public registries also encourage penal entrepreneurs (Feeley, 2002) who profit from and contribute to punitivity. For instance, the company OffenderWatch developed a proprietary software platform that "powers the state sex offender registry in 16 states and registries for local agencies in 38 states". OffenderWatch also provides its own form of credentialing, awarding "National Certificates of Excellence" to "law enforcement who most exemplify

the objectives of the Sex Offender Registry unit." (see https://www.offenderwatch.com/community-awards). Such a transfer of power to private actors not only invites profit motives into state operations but creates the potential for private companies to create and expand punitivity, motivated by commercial interests and aided by digital technologies (see Corda and Lageson, 2020). Along these lines, the technologically-driven surveillance of registries might also be usefully conceived through science and technology (STS) studies, centering the social construction of technologies and the power dynamics in both a tool's creation and effect (see, for instance, Troshynski, 2017).

Of course, what makes the registry unique in the punishment literature is the American legal designation of the registry as a civil and *non-punitive measure*. Our analysis here, supplemented by a 50-state survey of how the registry operates today, directly questions the enduring validity of this legal designation amidst a new technological backdrop. Recent sociolegal scholarship has squarely analyzed the relationship between technology and the criminal legal system (Brayne, 2021; Lageson, 2020; Lane, 2018; Stuart, 2020). We draw upon this line of substantive inquiry to frame the registry as not only a form of punishment, but as a uniquely digital punishment, given that registries live on the internet. Alongside the punishment functions of the registry, the digital format also allows for the expansion of both state surveillance and lateral surveillance (Andrejevic, 2004), an issue we explore through the specific website functionalities and capabilities that facilitate non-state surveillance and tracking.

In sum, a sociological analysis of the contemporary digital sex offense registry invokes questions of penal entrepreneurialism, surveillance and punishment. Legally, our observations raise new questions about the applicability of the *Smith v. Doe* standards in today's digital world. We next describe empirical efforts to code online registries, then describe our methodological approach to analyze registries' digital punishment and lateral surveillance qualities.

Analyses of online registries

Registry content has changed over time due, in part, to SORNA laws (Brewster et al., 2013; Harris et al., 2020a; Navarro and Shellabarger, 2023). In 2005, prior to SORNA, Tewksbury and Higgins conducted a content analysis of online sex offense registries and tracked 28 elements of registries across 40 states. They found great variability in the content contained on each state's online registry (Tewksbury and Higgins, 2005). Seven years after SORNA's passing, Mustaine and Tewksbury (2013) and Brewster et al. (2013) found that all 50 states now had online searchable registries and that the amount of information available about registrants and searchability functions had greatly expanded.

A system of federal incentives also expanded the technological capabilities of the registry. The Department of Justice monitors states for compliance with SORNA's call for a "comprehensive national system" for registration (see US DOJ, 2021). These initiatives have created interstate enforcement efforts, the establishment of new offices to oversee implementation, and improvements to information systems to promote the exchange of information between states and expand public access (Harris et al., 2020b). This also

meant an influx of federal resources to support states in compliance with SORNA, including Standard 10. The Office of Sex Offense Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART Office) was established to oversee implementation of the Act and manage resources available to states (Harris et al., 2020b). These include both competitive SORNA grant program funds and a 10% reduction in federal Justice Assistance Grant (JAG) funding for noncompliant states that can then be captured if states make an effort to comply (Harris et al., 2020b: 6, footnote 4). The funds have been utilized to "improve data quality, enhance technological capacity, expand registry enforcement efforts, and fulfill a range of other functions connected to the achievement of SORNA's goals" (Harris et al., 2020b: 6).

Three information technology initiatives have stemmed from the SMART Office: The Dru Sjodin National Sex Offender Public Website (NSOPW), the Sex Offender Registration Tool (SORT), and the SORNA Exchange Portal (SEP). Each of these supports the data sharing and collaborative linking of data across disparate state registry websites. According to Harris et al. (2020b), the NSOPW has enhanced its geographic search functionality and added a mobile phone application. The SORT provides states with a cheaper alternative to building their own registries by providing a "SORNA-calibrated" registration system that is positioned to integrate all state-run online registries into a linked network (Harris et al., 2020b: 7). Finally, the SEP offers a platform for the transfer of information across jurisdictions, further aiding in the integration of information from various jurisdictional registries (Harris et al. 2020b: 7). Collectively, these compliance efforts also result in the aggregation of data across time and place, an expansion in the scope of information available about people, and an enhancement in the ability for the public to digitally browse, map, track, and surveil those subject to registration requirements.

The most recent work establishing patterns across online registries is by Navarro and Shellabarger (2023) who coded all state registries across 88 indicators and then tested whether differences between states were attributable to federal pressure to standardize information across states. They find that heterogeneity continues to be a hallmark across states; specifically, "that registries continue to change, incorporating novel registry elements, primarily with how the public can disseminate registry data, registry search features, and the listing details of registrants and their offense information" (Navarro and Shellabarger, 2023: 501). But they also found that states that complied with federal guidelines were statistically more likely to disseminate more information about registrants than states that failed to meet Standard 10. We extend this empirical research by focusing specifically on digital surveillance capabilities, tying our observations to contradict the legal arguments set out in *Smith* and to clearly tie these arguments to the sociology of punishment.

Methods and data

Our empirical aim is to identify and report the current technological capabilities of state-run sex offense registries through a 50-state survey. We accompany our reporting of these digital trends with qualitative examples from state and private websites that show how registry data are repackaged and reproduced across the internet. These descriptive data sources are leveraged to make our broader argument: that today's sex offense

registry operates in a fundamentally different manner than the registry as understood by the Supreme Court in 2003.

Our dataset contains 14 indicators related to digital capabilities in sex offense registries. We did not begin coding state registry websites with narrowly defined data points; rather we began with an open coding approach that allowed us to evaluate the digital landscape. We then focused more intently on technological design aspects of the registry, such as user functionality additions like open browsing of registrants, the ability to download the registry as a bulk dataset, options to receive personal updates about specific registrants and/or share that information with a friend, and advanced geolocation and mapping capabilities. We ultimately developed a codebook of 14 indicators that we categorize into three typologies of surveillance. After we identified the state-run public registry for each state, we coded every state for each data point. We ultimately reviewed our entire dataset twice; discrepancies were noted and resolved through discussion until consensus.

It is important to note that these data represent a snapshot of each state's registry as it existed during data collection. As laws change and state resources, priorities, and responsibilities shift, the data collected in this database shifts as well. There were updates and changes to our data even in the year and a half of data collection. We are confident that these data serve as a useful tool to understand the nature of state sex offender registries as they operate today but we duly note the limitations inherent in this approach.

Our results lead to several key findings: 1) registries now regularly contain surveillance capabilities that allow users to browse, map, and track people on the registry; 2) in some states, registry information is automatically exported as bulk data and/or indexed by internet search engines; and 3) the private technology sector both works directly with and extends the power of the state by offering software platforms for state-run registries and creating private versions of registry data to internet users. This aid and expansion of state control means that internet users are "pushed" registry data, even when they are not actively seeking it—a stark contrast to how the registry was understood by the Supreme Court in its non-punitive, civil designation.

Analysis

Our analysis proceeds in two parts. First, we focus on indicators that contribute to the digital punishment and surveillance effects of the registry, and we categorize these elements as lateral surveillance, location surveillance, and data surveillance, but note there is overlapping qualities. Table 1 summarizes these themes and frequencies.

Lateral surveillance includes indicators for when the state offers specific technological capabilities that allow non-state actors to share information, sign up to receive updates, or directly submit a tip to law enforcement on the registry platform. These indicators reflect design choices where the state provides specific tools that increase civilian surveillance.

Location surveillance includes advanced mapping capabilities and address searching that bridge physical locations with digital tracking, allowing users to access state information and then utilize this information in physical spaces.

Table 1. Digital surveillance capabilities of sex offense registries in the U.S.

Lateral surveillance	Submit a tip function	27 (54%)
	Share with a friend function	15 (30%)
	Sign up for updates	33 (66%)
Location surveillance	Browsable map	36 (72%)
	Targeted address search	24 (48%)
Data surveillance	Broad name browsing	30 (60%)
	Targeted name search	19 (38%)
	Bulk download of registry	6 (12%)
	Search by internet identifier	13 (26%)
	Indexed by Google Search	11 (22%)

Data surveillance highlights how registries create digital information that is easily shared between state repositories and private data companies. Specifically, data surveillance occurs when state registries create functionalities that ease private sector access to information by allowing bulk data downloads or search engine indexing. The spread of personal information creates digital stigma as private sector actors use and market registry data in profit-seeking enterprises that further cement digital punishment and stigmatization (Table 1).

Lateral surveillance

Lateral surveillance is a form of "peer monitoring" (Andrejevic, 2004) or "deputization" (Brayne et al., 2023) that expands the state surveillance apparatus by inviting members of the public to participate. Over half of state registries allow users to sign up for updates pertaining to a specific person on the registry, where the state, for instance, will share with that user changes to the registered person's home address. Such tracking is not limited to those who have been harmed by the registered person, as in other victim notification schemes, but is instead a state service provided to any internet user from any jurisdiction. The Nebraska registry, for instance, allows a user to sign up for notifications regarding a specific person on the registry, and the North Dakota registry allows internet users to "track offender" (see Figure 1).

This option is often not available for other types of criminal history information made public by state or local government. For instance, people under probation supervision, even for violent crimes, are not posted to public registries that allow for active surveillance. Nor are people with prior conviction records or those awaiting criminal adjudication. Thus, the tracking functions of the registry select out these types of convictions as particularly dangerous and in need of constant and continuous supervision (see Figure 2).

Registries also allow users to share registrant information among their social networks; 30% of states provide a direct "share with a friend" function. While the registry can always be shared with other internet users by virtue of sharing a URL, this specific technological capability may encourage such sharing of information and widen the social surveillance apparatus, as displayed in Figure 3. Twenty-seven states also provide a direct link to submit a "tip" directly to the state, in a form of "surveillance deputization" of civilians now tasked with police surveillance work (see Brayne et al., 2023).

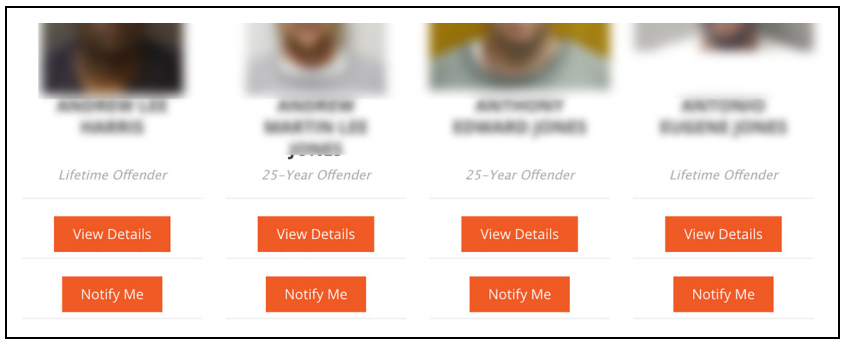


Figure 1. Screenshots from Nebraska Registry showing notification and tracking functionalities. Source: sor.nebraska.gov

Figure 2. The "Tell A Friend" function is offered by OffenderWatch and utilized on the Connecticut registry. Source: https://sheriffalerts.com/cap_main.php?office=54567.

The architecture and design of registries may also encourage public monitoring by highlighting people on the registry who have not recently verified their information and are thus considered "noncompliant" with state registry law. For instance, the Missouri registry reports whether a registrant is compliant and maintains a separate page of non-compliant registrants whose photos are rotated on the main webpage. The Tennessee registry similarly allows for tracking and information sharing options on its homepage, which also displays a grid of currently noncompliant registrants.

The registry thus allows for a highly interactive user experience that encourages and enables community surveillance efforts that aid state legal processes. Unlike the characterization of the registry in *Smith*, the interface, text, and tracking options on registry websites do not simply provide historical conviction information, but present registrants as presently dangerous and in need of public monitoring that expands beyond the bounds of the state agencies tasked with such work.

Figure 3. Data sharing functionalities are offered on the Iowa registry. Source: https://www.iowasexoffender.gov/search/.

Location surveillance: mapping people on the registry

Today's registries also allow internet users to browse maps and track individual registrants' locations, including both home addresses and (in some states) workplace addresses. Nearly 75% of states allow for users to map registrants' addresses through either open browsing of addresses across the state or a jurisdictional search. This expands the geolocation capabilities of the registry away from the home address of the internet user. Some states limit this functionality to only show the block or small radius within which a registrant is located while others provide a precise geolocation match for a registrant's address. This may include current and past addresses as well as employer and school addresses as well (for instance, Navarro and Shellabarger observed in 2023 that 10 states include work addresses and 10 states list school enrollment. Additionally, 24 states list employer address and 10 states list address of school). By utilizing widely accessible Google maps or ArcGIS platforms, registries provide geospatial representations of where people on the registry live. In the Missouri registry, an internet user who searches an address will see an interactive map of the location of all registrants within a specified radius. Aggregating results by location also allows for broad sweeps of downloadable registry information. For instance, users can enter a city, town, or neighborhood name to browse lists of registrants. That list can then be exported as a text file, which is easily pasted into a spreadsheet of registrant data, creating a bulk dataset (see Figures 4 and 5).

Data surveillance

Finally, design choices in registry website functionality enable the surveillance of personally identifiable information into bulk datasets that can be repurposed. For instance, 60%

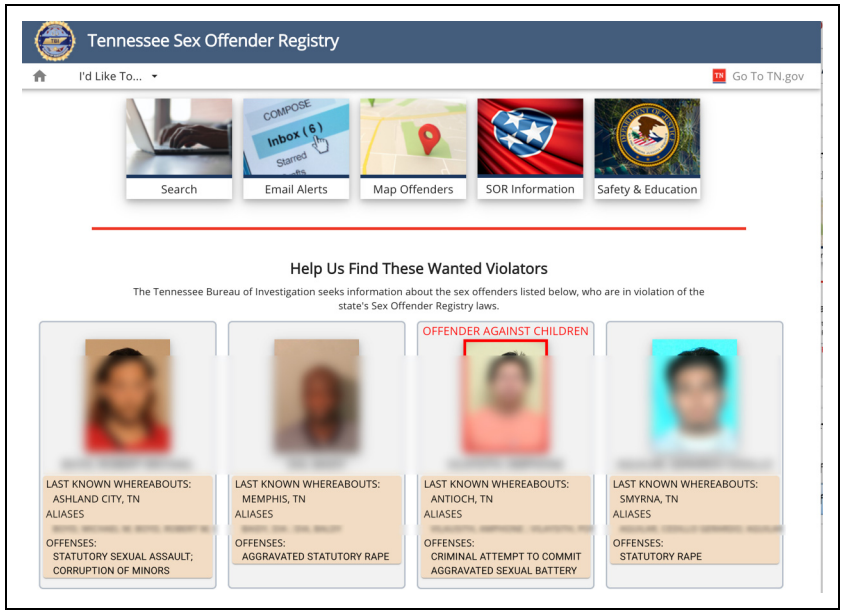


Figure 4. Search, alert, and information sharing options are provided by the Tennessee registry. Source: https://sor.tbi.tn.gov/home.

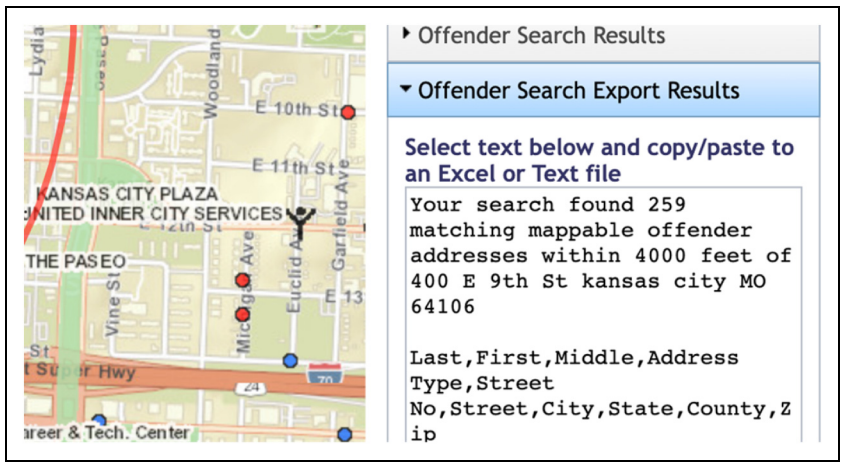


Figure 5. Screenshot of data export option for location based registry searches. Source: https://www.mshp.dps.missouri.gov/CJ38/AreaSearch.

of state registries allow for bulk searches; when entering only a single letter into the "name" search field, the website then retrieves every registrant whose name contains that letter. More than half of states (N = 30, or 60%) allow internet users to openly browse

or input one letter to return bulk search results of registrants on their online registries. Some states simplify the process by allowing for a simple download of the entire state's registry data file, such as in Figure 6 (Illinois, Missouri, Oregon, South Dakota, Texas, and Virginia). Rather than providing registry information as a searchable archive, this enables third parties to export all registrant data at no cost or accountability for secondary uses.

Registries also allow for searches beyond name and address. Thirteen states allow internet users to search for internet identifiers, such as email addresses. The Oklahoma registry allows searches by physical characteristics, including race, sex, age, height, or a text-based physical description (see Figure 7). The searchable database of registry information has expanded beyond name, photograph, and address, and now catalogs biometric data as well.

These data export and search functions are unlike the process outlined in *Smith*, where "an individual seeking the information must take the initial step of going to the Department of Public Safety's website, proceed to the sex offender registry, and then look up the desired information" (*Smith* at 99).

Further, these bulk data export capabilities create large swaths of data retrieved, copied, and disseminated by private third-party actors, contributing to digital stigma. Registry information, once put online, enters a Pandora's Box of digital data. This may happen by the state allowing the registry to be indexed by search engines so that routine

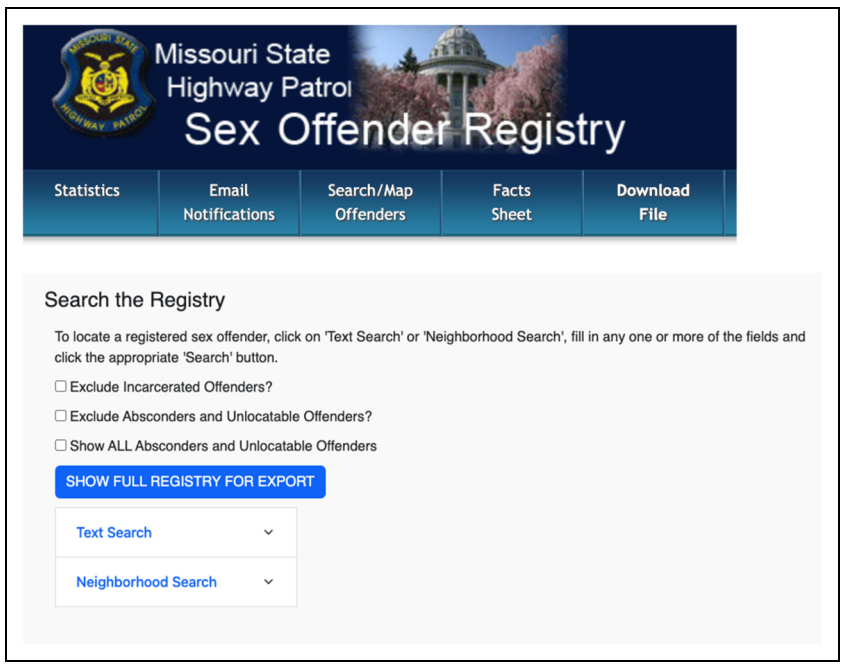


Figure 6. Download functionality on the Missouri and South Dakota registry websites.

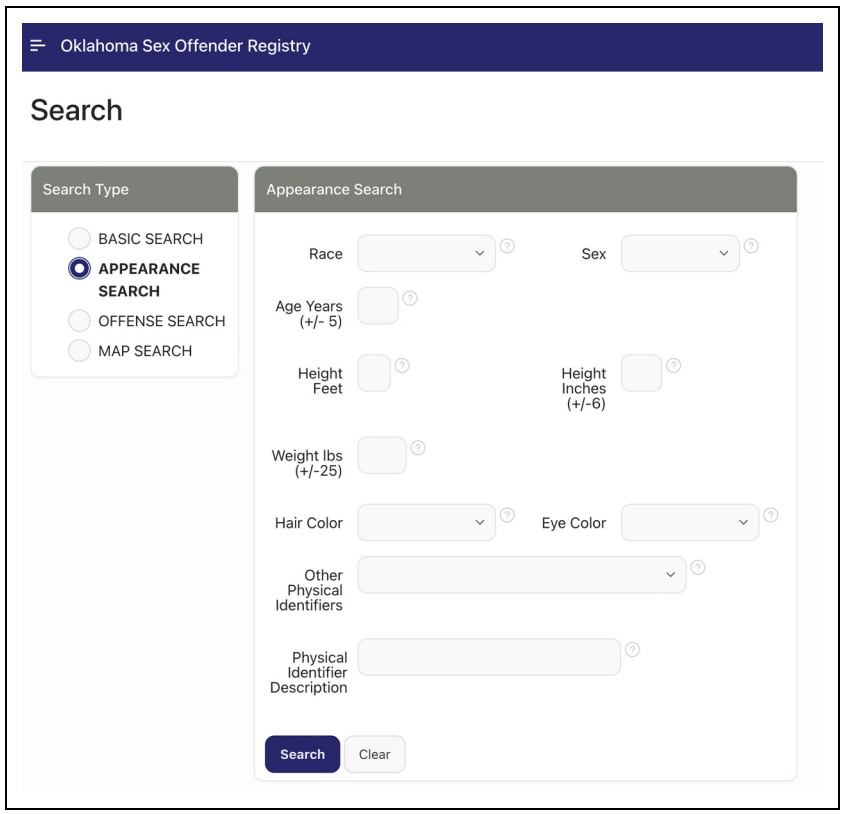


Figure 7. Oklahoma registry search functions. Source: https://sors.doc.ok.gov/ords/svorp/sors/r/sors/public-search.

internet searches for a name or address will return registry results, or by the state failing to limit data scraping. For instance, 11 registry websites are indexed by search engines. As "search engine spiders" continuously "crawl" public webpages, a basic Google search for that person's name will return a link to a governmental sex offender registry website. While websites have the option to block search engine crawlers that add content to search engine results, 22% of state registries allow indexing, which ensures the registrant's personal information contained in the registry appears in Google search results.

Search engine indexing has increased public access to registrants' personal information because the nature of such information is prioritized by internet search engine algorithms, frequently causing the registrant's status to end up among the top search results for a registrant's name. Search results are ranked by how often an internet user clicks a link. Due to the "shock value" of sex offender information in the search results for a person's name, links to websites that post registry information often maintain dominance as top results (Pierce, 2013). Addresses are similarly indexed into Google, so that a search for a home or business address may yield a link to the registry that inadvertently displays

a registrant's personal details. This may increase stigma by negatively and publicly marking those housing and employment sectors used by people on the registry. Internet users no longer have to seek out registry information by navigating to a state website; instead they can inadvertently learn a person is on a registry through a basic, generic internet search for a person or place. Search engine algorithms boost this type of information, multiplying access to a variety of sources that post registry data.

Penal entrepreneurialism & the data push of registry information to the public

Public records, including registrant information, are a valuable data commodity (Lageson, 2020). In particular, registrant information is used by websites that aggregate public records to create reports about people and places. In these largely unregulated web services, companies supply and display geo-specific registry information without a user ever making a specific request. Registry information is scraped from governmental sources and repackaged into a web product that is pushed to internet users.

For instance, Homefacts.com, a site that provides neighborhood information, supplies registrant information along with information about property prices and school ratings, such as this free Homefacts report (see Figure 8) about Des Moines that uses registry data as a key indicator of an area overview. Scrolling down the Homefacts webpage, a user is provided with a set of registrants, including their photographs and home addresses.

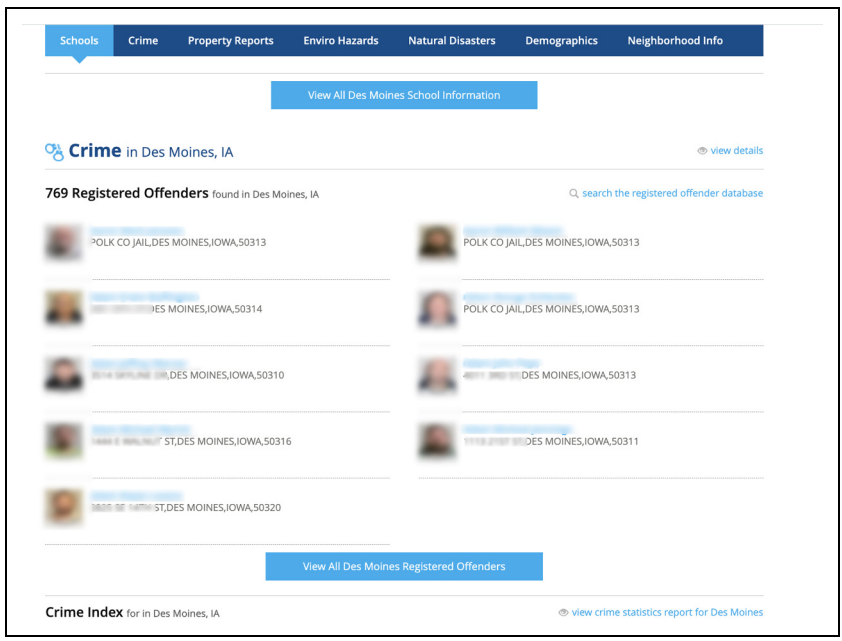


Figure 8. Homefacts.com use of registry information to create city assessment reports. Source: https://www.homefacts.com/city/Iowa/Polk-County/Des-Moines.html.

Other companies aggregate public records to sell "people search" reports to consumers. In these reports, companies now proactively include registrant information for people who live nearby the target of the search, pushing registrant data to internet users who are seeking information on a *different person* altogether. For instance, Instant Checkmate provides background reports that draw upon public records databases and report addresses, criminal histories, and social media accounts for the search target. However, Instant Checkmate also affirmatively posts registrant information for people who live in proximity to the search target. A sample Instant Checkmate report provided by the company displays the registrant data included on background check reports for non-registrants (see Figure 9).

Similarly, city-data.com offers a broad set of information about cities, towns, and zip codes, including population demographics, weather patterns, real estate taxes, tourist attractions, industries and occupations, and education. The site also offers its own sex offender locator, built directly into the website. Clicking on a search result reveals the name, home address, sex, age, eye color, hair color, height, weight, scars/marks/tattoos, and race of the registrant.

None of these private companies push or proactively provide criminal conviction information for any other type of criminal record, including violent crime or homicide. Nor do these third-party websites report any personal information about people with other criminal convictions, such as their home address or photograph. Instead, these websites only provide registry information, something which state-run websites facilitate by design.

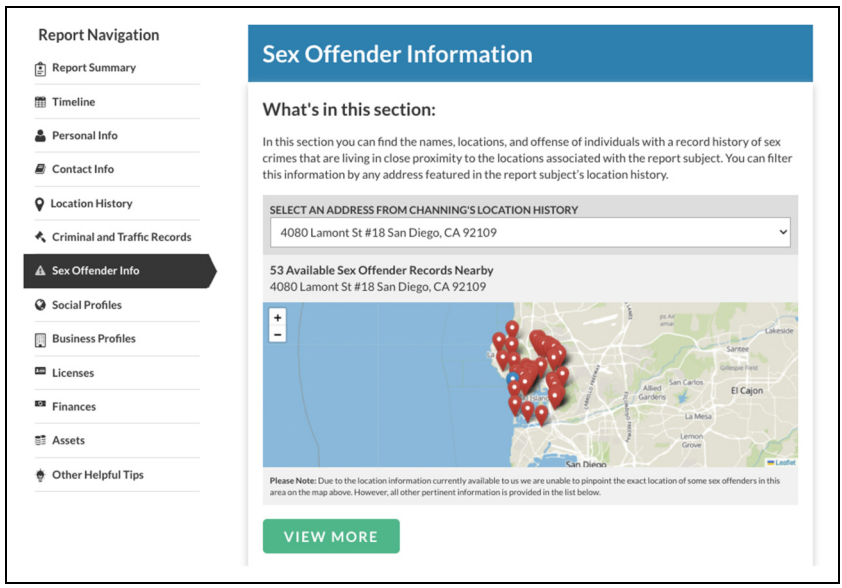


Figure 9. Sample Instant Checkmate report advertising integration of registrant photographs, offense, and link to purchase a background report. Source: https://www.instantcheckmate.com/crimewire/post/instant-checkmate-sample-report/.

Private entities also aggregate registrant information to create new, private databases of such information to generate income. Family-watchdog.us, for instance, is owned by an Indiana-based for-profit company called FWD Holdings that aggregates registry information from states and repackages it for internet users to their site. The website hosts advertisements and links to other for-profit records aggregators. For instance, a search result for an address reveals a map of registrants and includes an advertisement to the registrant's BeenVerified background check, an unregulated, for-profit people search service. Familywatchdog.us also provides sales packages to media entities, law enforcement agencies, and other private companies seeking to mine registry data or host maps or mobile applications showing the locations of registrants, effectively using public registrant information as a for-profit data commodity.

Discussion

Accessing registry data used to require an internet user to navigate to a government website and conduct a targeted search for information about a specific person with a sex offense conviction. Changes in internet infrastructure and database technology over the nearly two decades since *Smith v. Doe* have transformed registry information from a government-run source that a user had to intentionally access into a large scale, private-sector data commodity that is duplicated, aggregated, and pushed to innumerable internet users who passively receive registrant information without even intending to access it. The detailed and easily downloadable nature of the information provided in the registry in turn enables a growing ecosystem of private sector uses of registry data for surveillance, stigmatization and shaming purposes. Theoretically, our analysis shows how the digital registry constitutes a form of expressive punishment and risk management, but with outsized effect due to the sociolegal construction of dangerous and irredeemable "offenders" and profit-motivated private-sector redistribution of registry data to attract website traffic.

In *Smith*, the majority opinion described the process of accessing registrant information as "analogous to a visit to an official archive of criminal records than it is to a scheme forcing an offender to appear in public with some visible badge of past criminality" (*Smith* at 99). This characterization not only does not reflect how the registry operates today but also does not reflect how registrant information that is originally posted on a state registry is reproduced on the internet. Rather than requiring an internet user to seek out registrant information by accessing a governmental database or criminal record archive, this information is now routinely pushed or provided to web users even without their intent to access such records.

These state disclosures of data that allow for the ongoing monitoring of registrants—by not only the state, but by private actors—are then re-disseminated across the internet as they are cataloged, indexed, sold, and shared by third parties. A person's registry status becomes digitally linked to their name and is continuously retrievable via basic internet searches; indeed, it may be the first thing that will show up on a Google search of the person's name. Because registrants are required to actively report their personal information, websites contain not just historical conviction records, but continuously updated

information about exactly where a person lives and works, what they currently look like, and what vehicles they drive. Lateral surveillance is encouraged by state-run registries that allow for unfettered mapping, searching, and notification capabilities that encourage users to contribute to the dissemination of registry information.

In contrast to the registry, other forms of public criminal record information maintained by the state require a targeted search of a specific person, do not allow for the browsing of lists of convicted persons, and do not include mapping, tracking, or alert capabilities. For example, many states maintain a criminal court records internet portal that provides a summary of a person's legal history accessible only through a targeted search for that particular person (see Lageson et al., 2021). Unlike this historical records archive, the registry provides a constantly updated set of personal information about registrants, conveying that registrants pose a current serious public safety risk.

In other contexts, federal courts have recognized that the digital transformation has changed the practical realities of governmental records and individual privacy interests. In 2016, the Sixth Circuit noted that while the disclosure of booking photos twenty years ago was thought to do no harm, "the internet and social media have worked unpredictable changes in the way photographs are stored and shared" (*Detroit Free Press Inc. v. United States Dep't of Justice*, 829 F.3d 478, 486 (6th Cir. 2016)). Overruling a 1996 decision, this decision pointed to how changes in technology have reshaped an individual's privacy interests in materials related to their criminal proceedings, precisely because of the internet's permanent archive of such materials, with instant access by anyone from anywhere in the world. The *Smith* court operated in a different social and technological world. Deeming the registry a civil, non-punitive measure at the time perhaps made sense. But the added elements of registration in the digital age create digital punishment and an expansive public surveillance tool.

Conclusion

Punishment and society research has increasingly engaged with questions about how digital technologies have transformed, expanded, or altered punitivity. The American sex offense registry offers a key case study for this line of inquiry. The digital transformation has fundamentally altered the nature of the registry from the civil, non-punitive archives envisioned by the Supreme Court into sophisticated surveillance and punishment mechanisms that extend far beyond state control. The proliferation of lateral surveillance capabilities, location tracking, bulk data exports, and private sector commodification has created a digital punishment apparatus that operates through both governmental and civilian monitoring networks. While the legal framework continues to classify these registries as civil measures, the empirical evidence demonstrates how dramatically this has changed. More broadly, this analysis highlights the need for continually expanding theoretical frameworks that account for how technology transforms ostensibly civil policies into tools of digital punishment and perpetual surveillance.

ORCID iD

Sarah Lageson https://orcid.org/0000-0002-4108-4365

Ethical approval and informed consent statements

The Ethics Committee of Rutgers University waived the need for IRB approval for content analysis of publicly available websites.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Any other identifying information related to the authors and/or their institutions, funders, approval committees, etc, that might compromise anonymity.

N/A

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Data availability statement

Data are available from the authors by request.

References

Agan A and Prescott JJ (2021) Offenders and SORN laws. In: Logan W and Prescott JJ (eds) *Sex Offender Registration and Community Notification Laws: An Empirical Evaluation*. Cambridge: Cambridge University Press, 48–58.

Andrejevic M (2004) The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society* 2(4).

Brayne S (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.

Brayne S, Lageson SE and Levy K (2023) Surveillance deputies: when ordinary people surveil for the state. *Law & Society Review* 57(4): 462–488.

Brewster MP, DeLong PA and Moloney JT (2013) Sex offender registries: a content analysis. *Criminal Justice Policy Review* 24(6): 695–715.

Byrne T, Cashy J, Metraux S, et al. (2022) Association between registered sex offender status and risk of housing instability and homelessness among veterans. *Journal of Interpersonal Violence* 37(7-8): NP5818–NP5829.

Campbell MC and Schoenfeld H (2013) The transformation of America's penal order: a historicized political sociology of punishment. *American Journal of Sociology* 118(5): 1375–1423.

Cohen S (1985) *Visions of Social Control: Crime, Punishment and Classification*. Oxford: Polity Press.

Cooper WL (2025) These states are debating castration for sex crimes. Experts call it cruel and pointless. *The Marshall Project*, June 21. https://www.themarshallproject.org/2025/06/21/sex-offender-law-louisiana-castration-crime.

Corda A and Lageson SE (2020) Disordered punishment: workaround technologies of criminal records disclosure and the rise of a new penal entrepreneurialism. *The British Journal of Criminology* 60(2): 245–264.

Durkheim E (1900/1973) Two laws of penal evolution. Translated by T. Anthony Jones. *Economy and Society* 2(3): 285–308.

Feeley M and Simon J (1992) The new penology: notes on the emerging strategy of corrections and its implications. *Criminology; An Interdisciplinary Journal* 30: 449.

Feeley MM (2002) Entrepreneurs of punishment: the legacy of privatization. *Punishment & Society* 4(3): 321–344.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*. Pantheon Books.

Garland D (2001) *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press.

Garland D (2018) Theoretical advances and problems in the sociology of punishment. *Punishment & Society* 20(1): 8–33.

Goodman P, Page J and Phelps M (2017) *Breaking the Pendulum: The Long Struggle Over Criminal Justice*. Oxford University Press.

Harris AJ, Kras KR and Lobanov-Rostovsky C, et al. (2020a) States' SORNA implementation journeys: lessons learned and policy implications. *New Criminal Law Review* 23(3): 315–365.

Harris AJ, Kras KR and Lobanov-Rostovsky C, et al. (2020b) Information sharing and the role of sex offender registration and notification, National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.

Janus E (2006) *Failure to Protect*. Ithaca, NY: Cornell University Press.

Kernsmith PD, Craun SW and Foster J (2009) Public attitudes toward sexual offenders and sex offender registration. *Journal of Child Sexual Abuse* 18(3): 290–301.

Kozlowska H (2019) There's a global movement of Facebook vigilantes who hunt pedophiles. *Quartz.* https://qz.com/1671916/the-global-movement-of-facebook-vigilantes-who-hunt-pedophiles/.

Kruse AE and Skilbrei ML (2024) The monster and the self: taking on the monstrosity of sexual violations. *Punishment & Society* 26(5): 840–859.

Lageson SE (2020) *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. Oxford: Oxford University Press.

Lageson SE, Webster E and Sandoval JR (2021) Digitizing and disclosing personal data: the proliferation of state criminal records on the internet. *Law & Social Inquiry* 46(3): 635–665.

Lane J (2018) *The Digital Street*. Oxford University Press.

Leon CS, Buckridge M and Herdoíza M (2023) 'I'm scared to death to try it on my own': I-Poems and the complexities of religious housing support for people on the US sex offender registry. *Anti-Trafficking Review* 20: 142–160.

Leon CS and Kilmer AR (2023) "Secondary registrants": a new conceptualization of the spread of community control. *Punishment & Society* 25(3): 641–664.

Levenson JS (2008) Collateral consequences of sex offender residence restrictions. *Criminal Justice Studies* 21(2): 153–166.

Lussier P, Chouinard Thivierge S and Fréchette J, et al. (2024) Sex offender recidivism: some lessons learned from over 70 years of research. *Criminal Justice Review* 49(4): 413–452.

Lynch M (2002) Pedophiles and cyber-predators as contaminating forces: the language of disgust, pollution, and boundary invasions in federal debates on sex offender legislation. *Law and Social Inquiry* 27: 529–557.

Meiners ER (2016) *For the Children?: Protecting Innocence in a Carceral State*. University of Minnesota Press.

Melossi D and Pavarini M (1981) *The Prison and the Factory*. London: MacMillan.

Meloy ML, Miller SL and Curtis KM (2008) Making sense out of nonsense: the deconstruction of state-level sex offender residence restrictions. *American Journal of Criminal Justice* 33: 209–222.

Mustaine EE and Tewksbury R (2013) What can be learned from an online sex offender registry site? An eight-year follow-up. *Journal of Community Corrections* 23(1): 5–10.

Navarro JC and Shellabarger CL (2023) A content analysis of sex offender registries: the influence of the sex offender registration and notification act (SORNA) on registry information. *Criminal Justice Policy Review* 34(5): 488–505.

Nobles MR, Levenson JS and Youstin TJ (2012) Effectiveness of residence restrictions in preventing sex offense recidivism. *Crime and Delinquency* 58(4): 491–513.

Norman-Eady S (2006) Castration of sex offenders. OLR Research Report, Web.Pub. L. 109-248. https://www.cga.ct.gov/2006/rpt/2006-R-0183.htm.

Pew Research. (2024) Internet broadband fact sheet. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

Pierce D (2013) The SEO behind mugshot websites. In: *Cogney*. Available at: https://www.cogney.com.hk/blog/mugshot-seo/ (accessed 7 May 2025).

Pratt J (2000) Sex crimes and the new punitiveness. *Behavioral Sciences & the Law* 18(2-3): 135–151.

Przybylski R (2015) Recividism of adult sexual offenders. Office of Justice Programs SOMAPI Research Brief. https://smart.ojp.gov/somapi/chapter-5-adult-sex-offender-recidivism.

Purshouse J (2020) 'Paedophile hunters', criminal procedure, and fundamental human rights. *Journal of Law and Society* 47(3): 384–411.

Reed P (2017) Punishment beyond incarceration: the negative effects of sex offender registration and restrictions. *Journal of Law and Criminal Justice* 5(2): 16–30.

Regina J (2012) Accessed denied: imposing statutory penalties on sex offender who violate restricted internet access as a condition of probation. *Seton Hall Circuit Review* 4(187): 187–222.

Simon J (2007) *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford: Oxford University Press.

Spencer D and Ricciardelli R (2017) 'They're a very sick group of individuals': correctional officers, emotions, and sex offenders. *Theoretical Criminology* 21(3): 380–394.

Stuart F (2020) Code of the tweet: urban gang violence in the social media age. *Social Problems* 67(2): 191–207.

Tewksbury R (2005) Collateral consequences of sex offender registration. *Journal of Contemporary Criminal Justice* 21(1): 67–81.

Tewksbury R (2007) Exile at home: the unintended collateral consequences of sex offender residency restrictions. *Harvard Civil Rights-Civil Liberties Law Review* 42(2): 531–540.

Tewksbury R and Higgins G (2005) What can be learned from an online sex offender registry site? *Journal of Community Corrections* 14(3): 9–11.

Tewksbury R, Jennings WG and Zgoba KM (2012) A longitudinal examination of sex offender recidivism prior to and following the implementation of SORN. *Behavioral Sciences & the Law* 30(3): 308–328.

Tewksbury R and Zgoba K (2009) Perceptions and coping with punishment: how registered sex offenders respond to stress, internet restrictions, and the collateral consequences of registration. *International Journal of Offender Therapy and Comparative Criminology* 54(4): 537–551.

Toler A and Bedi N (2025) Pedophile hunting and the rise of vigilante violence in America. *The New York Times*, 26 March. Available at: https://www.nytimes.com/interactive/2025/03/26/us/pedophile-hunting-violence.html (accessed 7 May 2025).

Troshynski EI (2017) Stalked by the state: GPS surveillance technology and sex offender parolees. *Kriminologisches Journal* 49(2).

United States Department of Justice. (2021) 86 FR 69856: registration requirements under the sex offender registration and notification act.

United States Department of Justice. (n.d.) SMART Office of sex offender sentencing, monitoring, apprehending, registering and tracking. Frequently Asked Questions. https://smart.ojp.gov/faqs#11-0.

Vogler S (2018) Constituting the 'sexually violent predator': law, forensic psychology, and the adjudication of risk. *Theoretical Criminology* 23(4): 509–526.

Vogler S (2021) *Sorting Sexualities: Expertise and the Politics of Legal Classification*. University of Chicago Press.

Walker JT (2007) Eliminate residency restrictions for sex offenders: special issue devoted to policy. *Criminology & Public Policy* 6(4): 863–870.

Werth R (2023) More than monsters: penal imaginaries and the specter of the dangerous sex offender. *Punishment & Society* 25(4): 977–997.

Williams M (2018) *The Sex Offender Housing Dilemma*. New York: New York University Press.

Wright R (ed.) (2014) *Sex Offender Laws: Failed Policies, New Directions*. Springer Publishing Company.

Yung CR (2007) Banishment by a thousand laws: residency restrictions on sex offenders. *Washington University Law Review* 85: 101.

Sarah Lageson is an Associate Professor in the School of Criminology and Criminal Justice and the School of Law at Northeastern University. Her research examines technology, inequality, and law.

Chloé Sudduth is a PhD Candidate in Criminology at Rutgers University-Newark. Her research examines digital technologies and the experience and consequences of punishment in contemporary society.