The Annual Review of Interdisciplinary Justice Research Volume 9, 2020

Edited by
Steven Kohm, Kevin Walby,
Kelly Gorkoff, and Katharina Maier
The University of Winnipeg
Centre for Interdisciplinary Justice Studies (CIJS)
ISSN 1925-2420

Research Note: "Privacy Loss as a Collateral Consequence"

Sarah Esther Lageson
Rutgers University

Abstract

The digital age has raised important new questions about privacy rights, particularly in the collection and dissemination of personally identifiable data. In a justice context, these privacy questions are compounded by the stigmatizing nature of criminal records. While discrimination based on a criminal conviction has been long documented in social science research, and privacy conversations have been invoked in criminal record policy, less direct attention has been paid to the psychological and social privacy harms of internet-based criminal record disclosure, especially for non-conviction, sealed, and expunged records. This note situates digital and reputational harms amidst broader collateral consequences of criminal records by discussing the complexity of competing privacy norms and law and the racialized dynamics of digital records and surveillance. By focusing on reputation and privacy, this note suggests that public policy better incorporate protections for the accused against digital punishment.

Introduction

In a digitized world, criminal records are increasingly available at a keystroke to employers, landlords, and a curious public. Though this phenomenon is well documented in the United States, the digital release of police and court records has also been documented in Canada (Bailey & Burkell, 2013), the United Kingdom, and Sweden (Corda & Lageson, 2019). While criminal records, particularly court proceedings, are made public in the interest of government transparency, these records also contain multitudes of personal information about arrestees and defendants, including full names, birthdates, and addresses. The rise of personal information in public criminal records has brought troubling consequences for people who

have been arrested or charged with crimes, especially for those offenses that have been dismissed or expunged. And while there are efforts to regulate criminal record–based discrimination and public shaming (such as in the United States' Clean Slate efforts and Europe's Right to Be Forgotten online), there has been less discussion of how internet reputation and digital privacy rights should be addressed specifically within a criminal justice context, especially when data is classified as a public record and includes pre-conviction information. Given the availability of such records, this note considers the need to incorporate privacy as a collateral consequence of justice system interactions that take into account dynamics of inequality, surveillance, and due process rights.

Digitization, Disclosure, and Harms

Criminal justice records used to exist in practical obscurity in the drawers and basements of police departments and courthouses, but the digital revolution has dramatically changed this scenario, especially in the United States, making even the most minor of criminal accusations part of the public canon, easily searchable and retrievable through the internet. In America, the 1996 Electronic Freedom of Information Act encouraged government agencies to "use new technology to enhance public access to agency records and information." This legislation was followed by the E-Government Act of 2002, requiring online access to federal court records, and leading state courts to follow suit. Legally, the records of criminal justice proceedings are considered a public good and retrievable through the Freedom of Information Act (FOIA) and transparency laws that govern law enforcement, courts, and correctional facilities in America. The practical obscurity of paper-based records in some ways undermined the promise of FOIA — but it also offered subjects a degree of privacy by limiting access to records to people who were willing to make the effort to request records.

As a result, documents pertaining to a variety of criminal justice operations are now available on the internet. For instance, in the United States, a daily record of police arrests and jail inmate rosters have long been part of the public record as a way to monitor arrests. But these records also contain a tremendous amount of information

about the arrested suspect, such as their name, address, and photograph. For court records, there is a common law right to "access court records to inspect and to copy" (*Nixon v Warner Communications, Inc,* 435 U.S. 589 [1978]) in the United States, and with varying degrees of public access in Canada and Scandinavia. These records too contain lots of personal information about defendants, including bail amount, home address, or date of birth.

But when they existed only on paper, the damage to reputation was minor. The emergence of big data approaches to the personal information industry, alongside broad digitization, duplication, and online indexing of these records, has fundamentally changed their scope. As a result, however, this dramatically changed the reach of records from being an item a person had to *actively* seek out in person to a bit of information one can *inadvertently* discover through a Google search.

Criminal record data constitutes an especially damaging type of personal data, given that it brings a particular type of stigma. Further, the various forms of criminal records available today include a broad swath of data, including booking photos, jailhouse rosters, court records, and prisoner databases, are routinely bought and sold by data brokers and background check vendors (Solove, 2002; Conley et al., 2011). Even in the rare cases where expungement could seal a governmental record, these privately sourced records remain online unless the record subject identifies each source and serves their expungement order to the website publisher of every online platform that features their mugshot or criminal record.

A long line of research shows how criminal records impact people's lives, establishing the "collateral consequences" of a criminal record (Hagan & Dinovitzer, 1999; Pinard, 2010; Justice Centre, 2018). These harms are referred to as collateral consequences because they are located outside the criminal legal system and implemented by non–criminal justice institutions (Uggen & Stewart, 2015). Criminal records regulate access and opportunity across numerous social, economic, and political domains (Pager, 2008). Surveys and experimental audits of employers measure the discriminatory impact of a criminal record on hiring outcomes; in sociologist Devah Pager's

Milwaukee-based audit study, pairs of "testers" were sent to apply for entry-level jobs — one applicant with a criminal record and one (otherwise identical) applicant without such a record. Pager found that for white testers, there was a large and significant effect of criminal record on employment: 34% of whites without records received callbacks, while 17% with records received callbacks. For black testers, 14% without criminal records received callbacks, compared to 5% with a record. Thus, the effect of a criminal record is "40% larger for blacks than for whites," though men from both race groups faced significant discrimination based on their felony conviction (Pager, 2003). Subsequent research has showed that this discriminatory effect also occurs for non-conviction arrest records, in ways similarly patterned by race (Uggen et al., 2014).

Criminal records can also impact a person's ability to secure housing (Carey, 2004/5), especially for those groups already facing discrimination from landlords in more vulnerable housing markets (Roscigno, Karafin, & Tester, 2009). The marketplace for court-ordered eviction databases is rapidly growing (TransUnion SmartMove, 2018), incorporating secondary criminal record information, such as arrests (American Information Research Services, 2018). For instance, AIRS (American Information Research Services, Inc.) sells landlords access to an eviction database that uses publicly accessible data, including criminal records, that they pull using "data retrieval services from public records sources only" (American Information Research Services, 2018). Landlords can run quick, free searches and "deny tenants housing based on the few (sometimes inaccurate or misleading) facts they find online" (Caramello & Mahlberg, 2017). Digital criminal record disclosure has also been shown to produce a particularly harmful chilling effect on prosocial behaviors, such as volunteering and parenting (Lageson, 2016).

While these types of discrimination have been addressed by various types of public policy and regulation (such as limiting an employer's ability to use arrest records, laws for expungement and record sealing, and regulating background checks through the United States Fair Credit Reporting Act), the attendant reputational harms caused by record disclosure have not been examined or addressed in similar

depth. Privacy theory offers a helpful starting lens to understand the social and psychological harms of record disclosure.

Privacy Theory

In Canada, the right to privacy has been codified through government regulation (such as the 1983 Privacy Act) and further cemented in case law, such as in the 1988 Supreme Court of Canada Case, *R. v. Dymet*, where the court noted that the right to privacy "must be interpreted in a broad and liberal manner" and that "its spirit must not be constrained by narrow legalistic classifications based on notions of property and the like which served to protect this fundamental human value in earlier times." In Europe, the right to privacy is defined as a fundamental right, alongside the freedoms of expression and association. In contrast, the U.S. Constitution does not address privacy as a fundamental right. Instead, courts have defined this right through case law as "penumbral," where privacy is located in the shadows of the First, Third, Fourth, Fifth, and Ninth Amendments of the American Bill of Rights. Thus, when privacy is questioned, courts draw from more clearly articulated rights to develop a modern concept of privacy that encompasses the contradictory guarantees of transparency in government and fundamental individual rights of life, liberty, and the pursuit of happiness.

The concept of privacy has evolved over time, often in tandem with technological changes that gave governments and companies more power to collect and leverage personal data about people. Originally, the concept of privacy carried connotations of feelings of loneliness or isolation (Glenn, 2003), but Enlightenment-era thinking ushered in a more rights-focused view of privacy that associated the concept with the relationship between the individual and the state. As time when on, privacy became equated with autonomy, choice, and liberty, or as Judge Thomas Cooley defined it in the 1880s, "a right of complete immunity: to be let alone" (Cooley, 1880), a phrase also adopted by American justices Samuel Warren and Louis Brandeis in their key 1890 *Harvard Law Review* article, "The Right to Privacy" (Warren & Brandeis, 1890). Anticipating the acceleration of new communication technologies that could transform "whisper[s] in the closet" to messages now able to be "proclaimed from the house-

tops," Warren and Brandeis also offered the idea of privacy as a right to control information about oneself as a mode of selective self-presentation, laying the groundwork for future, legal concepts of digital and reputational privacy (Warren & Brandeis, 1890, 195).

Academic considerations of privacy also accelerated as concerns over data privacy and surveillance loomed larger. In legal academia, the digital transformation ushered in a rich body of work analyzing identity and privacy issues in a technologically mediated world. With a focus on how digital information is created and attached to people, legal scholar Jeffrey Rosen (2000) writes of the "unwanted gaze" of data-driven surveillance that observes and records our digital identity, combining disparate pieces of information from a variety of sources and stripping these data from their original context, and then using this information against people. This leaves us "vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences" (Rosen, 2000, p. 9). Daniel Solove (2002) agrees, describing the creation of "digital biographies" as an "unauthorized biography, only partially true and very reductive," pointing to an "aggregation problem" (p. 1137). When we allow government to share our data freely with private companies that haphazardly combine various information sources, the result is a "growing dehumanization, powerlessness, and vulnerability for individuals" (Solove, 2002, p. 1140). Digital personal information, posits Helen Nissenbaum, should be understood and evaluated by its "contextual integrity," which forces attention to the nuances of data, such as the subject, sender, recipient, information type, and mode of transmission (2009).

Social scientists have wrestled with how to understand privacy in various social contexts, how to incorporate social structure and inequality into privacy rights, and how to establish a solid legal ground for controlling personal information (Baghai, 2012). This view posits privacy as a "resource that is unequally distributed in society," which in turn means that the "production and management of privacy may create inequality among social actors" (Anthony et al., 2017, p. 15). Emerging sociological and criminological conceptions of privacy, then, not only ask questions about individual autonomy and control over one's personal information, but also about

access and equity to privacy rights at all.

Privacy Violations and Avoidance

Privacy violations create a chilling effect on people's behaviour, which is often a basis for the articulation of privacy rights. Organizations like the Privacy Rights Clearinghouse in California assert that, when a person's privacy is violated, they begin to avoid situations where personal information is gathered, effectively avoiding participation in civic and public life to try to control their information (Privacy Rights Clearinghouse, 2002). Research has shown this to be true within the criminal justice context, with studies showing that people with criminal histories purposefully "opt out" of prosocial situations, such as volunteering and voting (Bernburg & Krohn, 2003; Carey, 2004/5; Pager, 2008; Winnick & Bodkin, 2008; Thatcher, 2008; Uggen et al., 2014; Uggen & Stewart, 2015; Lageson, 2016).

Technology exacerbates these effects. Inequality researchers show that low-income people face a "matrix of vulnerabilities" as result of the collection and aggregation of big data (Madden et al., 2017), especially in their ability to protect personal information online, prevent digital privacy harms, and police their online persona. While privacy concerns are central to debates over how personal information is swept into technological transformations of society, the ability to exercise privacy is too often a privileged right. Sociologists have conceptualized privacy as access of one actor to another, making access a valuable resource in a field (Anthony et al., 2017). This might include access to information, access to particular types of information, and the ability to use information in particular ways, calling into question how privacy and access intersect with power, especially in a punitive institution like criminal justice.

Discovering one's own online criminal stigma can be shocking, surprising, and upsetting to the criminal record subject. Confronting digital criminal record stigma can lead to an attempt to "fly under the radar" to avoid having others discover the information (Lageson, 2016). This is akin to other forms of institutional avoidance documented in criminal justice research, such as in Goffman's

observation in her Philadelphia study of young men who purposefully avoided places, relationships, stable routines, and legal services as a method to "cultivate unpredictability" and avoid the threat of police contact (Goffman, 2015). Similarly, by introducing the concept of "system avoidance," Brayne (2014) quantitatively assesses these avoidance patterns documented in qualitative research. Her analysis shows that people with criminal justice experience are less likely to interact with "surveilling institutions," including medical, financial, labour market, and educational institutions. Having a multitude of online criminal records has a similar contribution to systems avoidance, and extends these avoidance techniques into digital spaces. By indiscriminately attaching stigma, online criminal records lead people to purposefully avoid situations that might induce an internet search for their name. This means avoiding participation in social and civic institutions or staying locked into less-than-desirable employment, housing, and relationships (Lageson, 2016).

The release and commodification of criminal records (particularly in the United States, but emerging in Canada and Europe [Corda & Lageson, 2019]) is potentially so widespread as to make privacy nearly impossible once a person is arrested, even if charges are never filed. At the same time, privacy violations — such as the public application of the criminal label — can be cause for people to disengage from digital and real-world contexts. In this way, the internet mimics the everyday experiences of disenfranchised people, becoming another system in which people do not have power or control over their representation.

Further, having the skillset and legal understanding required to claim privacy equity involves having access to a set of resources, privileges, and a particular type of legal consciousness. The outcome is that those *least* likely to be entangled in the criminal justice system are often best equipped to deal with the privacy and reputational impacts. Implicit in the structure of "digital punishment" is a predetermination of who gets to move on from an accusation, arrest, or conviction, and truly get the second chance promised in the proverbial rehabilitative aim of the criminal justice system (Lageson, 2020). Patterns of social and racial inequality in criminal justice operations are thus compounded into privacy inequalities, structuring

the impact of privacy harms to disadvantage those who are most vulnerable. Not only does digital punishment unequally stigmatize marginalized and socially ostracized groups, it exacerbates privacy inequalities because members of these already sidelined communities are less likely to have the ability to address, remedy, or overcome a criminal record (Myrick, 2013). Mass punishment is raced and classed at its roots, and thus it should come as no surprise that its offshoot, digital punishment, is so raced and classed as well.

Preservation and Identity

In the United States, there is concern that attaching privacy rights to the accused will undermine the notion of the public record. The blurred line between public records and technology companies has further complicated this matter as private companies monetize and publish personal information online. In contrast to the American system of allowing private companies to disseminate public records that are indexed into internet search engines, Europe has regulated privacy and identity through regulating technology companies and search results (including criminal records) though "Right to Be Forgotten" legislation. To further strengthen these privacy protections, most European countries restrict access to both pre- and post-conviction records of criminal processing (Jacobs & Larrauri, 2012).

In contrast, American governments opt for disclosure of criminal records, and American tech companies typically disagree with the Right to Be Forgotten. For instance, Google immediately challenged the EU ruling in a *Guardian* op-ed and argued that forcing the search engine to remove links "means that the *Guardian* could have an article on its website about an individual that's perfectly legal, but we might not legally be able to show links to it in our results when you search for that person's name. It is a bit like saying the book can stay in the library but cannot be included in the library's card catalogue" (Drummond, 2014). The *New York Times* editorialized that "the European position is deeply troubling because it could lead to censorship by public officials who want to whitewash the past. It also sets a terrible example for officials in other countries who might also want to demand that Internet companies remove links they don't like"

(The Editorial Board, 2015). Eugene Volokh (2017) wrote in the *Washington Post* that such a law is "unconstitutional under current First Amendment law, and I hope First Amendment law will stay that way (no matter what rules other countries might have adopted)."

These public pronouncements don't match neatly with public opinion; a 2018 poll found nearly nine in ten Americans support Right to Be Forgotten legislation in the United States (Trujillo, 2018), likely because people inherently seek control over their online identities. But when tech companies and First Amendment advocates like Volokh invoke the positive aspects of the United States having the right to publish and link to criminal records, he is implicitly drawing a broader cultural line between America, Canada, and Europe. He unwittingly demonstrates how cultural norms shape the development and application of privacy law, as well as the broader understandings of technology and its role in society. In this sense, the Right to Be Forgotten addresses what some see as a core philosophical divide between Europe and the United States regarding how digital information should be treated. The American view often posits that once information is online it should stay online, taking a preservationist approach that stands in contrast to a "deletionist" approach, which argues preservation and permanence represent an unrealistic view of how human memory works (Jones 2016, p. 102). Instead, the deletionist view posits, information is at the mercy of malleable processes of shifting memories and the passage of time. Viktor Mayer-Schönberger (2011), for instance, argues that digital documentation negates time, and argues that through "perfect memory, we may lose a fundamental human capacity — to live in the present" (p. 12). And digital memory, claims Meg Leta Jones (2016), "prevents society from moving beyond the past because it cannot forget the past" (p. 20). Privacy scholar Julia Powles (2015) agrees, arguing that a preservationist approach is "insufficiently nuanced to cope with the reality of our lives and the complexities of human existence … Since when has the internet become 'truth', or 'memory?' And since when has 'history' been reduced to Google's commercially prioritised list of an imperfect collection of digital traces?"

Rehabilitation, Privacy and Collateral Consequences

In many ways, technological innovation within the criminal justice system can be harnessed for positive ends. Transparency policy allows for governmental watchdogging. In the aggregate, data about police and courts can uncover systematic discrimination and bias and lead to better justice outcomes. DNA testing can exonerate an innocent person, facial recognition software can be used to identify victims of sex trafficking, and body-worn cameras can improve police accountability. But the reputational harms of criminal record disclosure do have real and lasting effects. People whose records are publicly disclosed on the internet have little recourse, particularly in the United States, and instead are forced to resort to digital and social avoidance as a response to privacy violations. The power to apply the criminal label now comes from many sources, including social media and crime watch websites, making stigma even more inescapable.

Plus, compilation, digitization, and availability of criminal records began to produce more public demand for records. This coincided with the rise of criminal justice operations, culminating in the era of mass incarceration of the 1990s and 2000s. Criminal record policy also grew more punitive. Sex offender registries, public notification laws, and the dissemination of records by both the public and private sectors are all symbols of a public that is ready and willing to single out criminal offenders and ensure that this label endures, even if these are shown to be ineffective or to carry unintended consequences. Megan's Law, passed in 1996, requires states to provide public notification of the identities and addresses of people convicted of sex offenses, but has shown mixed results when it comes to actually preventing crime. Registries may even increase recidivism.

Granting access to criminal records is a steadily popular political talking point, framed as a method for ensuring public safety. Yet, the criminal label has been shown to be largely ineffective for preventing crime, and in some ways can be criminogenic by hindering rehabilitation, leading to a so-called self-fulfilling prophecy (Lageson & Maruna, 2018). Public policy debates moving forward might focus on more centralized management of pre-conviction and court processing data, or limit the inclusion of private data brokers that

mine, duplicate, and sell criminal record data in the United States, Canada, and Europe. As concern over data privacy continues to grow, the time may also be ripe for criminal record reform, particularly amidst debates in the United States over increasingly popular "Clean Slate" record expungement policy.

In considering the consequences of criminal punishment, it is imperative to now include reputational and privacy harms amidst the growing list of collateral consequences of a criminal record. It is also key to situate the rather rapid growth of digital criminal record disclosure among other forms of "tough on crime" rhetoric that favours perpetual, public punishment. Reputational punishment has always been part of the broader punishment apparatus, but the net of people swept into such harms has grown far beyond those convicted of sex offenses or other high-profile crimes. Digital and informational harms are remarkably expansive by initiating data surveillance and privacy harms at the moment of an initial police contact and extending far beyond the payment of a fine or serving a jail or prison sentence. By attaching stigma at so many points across the justice system, these digital privacy harms are permanently stigmatizing as criminal records become a lingering part of the internet archive.

References

American Information Research Services, Inc. (2018). Bulk eviction database. Accessed June 2, 2018, http://amer-info.com/our-services/bulk-eviction-database/.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology* 43: 249-269.

Baghai, K. (2012). Privacy as a human right: A sociological theory. *British Sociological Association* 46(5): 951-965.

Bailey, J., & Burkell, J. (2013). Implementing technology in the justice sector: A Canadian perspective. *Canadian Journal of Law and Technology*, 11(2): 253-282.

Bernburg, J.G., & Krohn, M.D. (2003). Labeling, life chances, and adult Crime: The direct and indirect effects of official intervention in adolescence on crime in early adulthood. *Criminology* 41(4): 1287-1318.

Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review* 79(3): 367-391.

Caramello, E., & Mahlberg, N. (2017). Combating tenant blacklisting based on housing court records: A survey of approaches. *Clearing House Community,* September 2017. Available at: http://povertylaw.org/clearinghouse/article/blacklisting.

Carey, C.A. (2004/5). No second chance: People with criminal records denied access to public housing. *University of Toledo Law Review* 36: 545-594.

Conley, A., Datta, A., Nissenbaum, H., & Sharma, D. (2011). Sustaining privacy and open justice in the transition to online court records: A multidisciplinary inquiry. *Maryland Law Review* 71(3): 772-847.

Cooley, T.M. (1880). *The law of torts* (1st ed.) University of Michigan Law School.

Corda, A., & Lageson, S. (2019). Disordered punishment: Workaround technologies of criminal records disclosure and the rise of a new penal entrepreneurialism. Forthcoming in *The British Journal of Criminology*. https://doi.org/10.1093/bjc/azz039.

Drummond, D. (2014). We need to talk about the right to be forgotten. *The Guardian,* 10 July. Available at: http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate (accessed 15 July 2017).

E-Government Act of 2002, 107 P.L. 347, 116 Stat. 2899

Electronic Freedom of Information Act Amendments of 1996, 1996 Enacted H.R. 3802, 104 Enacted H.R. 3802, 110 Stat. 3048

Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681

Glenn, R.A. (2003). *The right to privacy: Rights and liberties under the law*. ABC-CLIO.

Goffman, A. (2015). *On the run: Fugitive life in an American city*. Picador.

Hagan, J., & Dinovitzer, R. (1999). Collateral consequences of imprisonment for children, communities, and prisoners. *Crime and Justice* 26: 121-162.

Jacobs, J.B, & and Larrauri, E. (2012). Are criminal convictions a public matter? The USA and Spain. *Punishment & Society* 14(1): 3-28.

Jones, M.L. (2016). *Ctrl+Z: The Right to be Forgotten.* New York: NYU Press.

Lageson, S. (2020). *Digital Punishment: Privacy, stigma, and the harms of data-driven criminal justice.* Oxford: Oxford University Press.

Lageson, S. (2016). Found out and opting out: The consequences of online criminal records for families. *The ANNALS of the American Academy of Political and Social Science* 665(1): 127-141.

Lageson, S., & Maruna, S. (2018). Digital degradation: Stigma management in the internet age. *Punishment & Society* 20(1): 113-133.

Madden, M., Gilman, M.E., Levy, K., & Marwick, A.E. (2017). Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review* 95: 53-125.

Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age.* Princeton University Press.

Myrick, M. (2013). Facing your criminal record: Expungement and the collateral problem of wrongfully represented self. *Law and*

Society Review 47(1): 73-104.

Nissenbaum, H. (2009), *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nixon v. Warner Communications, Inc, 435 U.S. 589 (1978).

Pager, D. (2008). *Marked: Race, crime, and finding work in an era of mass incarceration*. University of Chicago Press.

Pager, D. (2003). The mark of a criminal record. *American Journal of Sociology* 108(5): 937-975.

Pinard, M. (2010). Collateral consequences of criminal convictions: Confronting issues of race and dignity. *NYU Law Review* 85: 457-534.

Powles, J. (2015). How Google determined our right to be forgotten. *The Guardian,* February 18 2015, https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search.

Privacy Act (R.S.C., 1985, c. P-21)

Privacy Rights Clearinghouse. (2002). Public records on the internet: The privacy dilemma. April 19, 2002. https://www.privacyrights.org/blog/public-records-internet-privacy-dilemma.

R v Dyment, [1988] 2 S.C.R. 417

Roscigno, V.J., Karafin, D.L., & Tester, G. (2009). The complexities and processes of racial housing discrimination. *Social Problems* 56(1): 46-69.

Rosen, J. (2000). *The Unwanted gaze*. Vintage.

Solove, D.J. (2002). Access and aggregation: Privacy, public records, and the Constitution. *Minnesota Law Review* 1137(86): 1137-1209.

Thatcher, D. (2008). The rise of criminal background screening in rental housing. *Law and Social Inquiry* 33 (1): 5-30.

The Editorial Board. (2015). Europe's expanding 'right to be forgotten.' *The New York Times,* February 4, 2015. https://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html.

TransUnion SmartMove. (2020). Eviction Report. Accessed March 9, 2020. https://www.mysmartmove.com/

Trujillo, M. (2018). Public wants 'right to be forgotten' online. *The Hill,* accessed 20 August 2018. https://www.bsgco.com/insights/public-wants-right-to-be-forgotten-online.

Uggen, C., & Stewart, R. (2015). Piling on: Collateral consequences and community supervision. *Minnesota Law Review* 99(5):1871-1910.

Uggen, C., Vuolo, M., Lageson, S., Ruhland, E., & Whitham, H.K. (2014). The edge of stigma: An experimental audit of the effects of low-level criminal records on employment. *Criminology* 52(4): 627-654.

Volokh, E. (2017). NY bill would require people to remove 'inaccurate,' 'irrelevant,' 'inadequate,' or 'excessive' statements about others. *The New York Times,* March 15 2017. https://www.washingtonpost.com/amphtml/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others/.

Warren, S.D., & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review* 4(5): 193-220.

Winnick, T.A., & Bodkin, M. (2008). Anticipated stigma and stigma management among those to be labeled 'ex-con'. *Deviant Behavior* 29(4): 295-333.