Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism

Corda, A., & Lageson, S. E. (2020). Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism. *British Journal of Criminology*, *60*(2), 245-264. https://doi.org/10.1093/bjc/azz039

Published in:
British Journal of Criminology

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

DISORDERED PUNISHMENT: WORKAROUND TECHNOLOGIES OF CRIMINAL RECORDS DISCLOSURE AND THE RISE OF A NEW PENAL ENTREPRENEURIALISM

Alessandro Corda[1] and Sarah E. Lageson

The privatization of punishment is a well-established phenomenon in modern criminal justice operations. Less understood are the market and technological forces that have dramatically reshaped the creation and sharing of criminal record data in recent years. Analysing trends in both the United States and Europe, we argue that this massive shift is cause to reconceptualize theories of penal entrepreneurialism to more directly address the role of technology and commercial interests. Criminal records, or proxies for them, are now actively produced and managed by third parties via corporate decision-making processes, rather than government dictating boundaries or outsourcing duties to private actors. This has led to what we term 'disordered punishment', imposed unevenly and inconsistently across multiple platforms, increasingly difficult for both government and individuals to control.

Key Words: criminal records, punishment and technology, privatization, digital age, penal entrepreneurialism

Introduction

Different sensibilities and approaches to the availability and dissemination of criminal records substantially affect people's lives. This is true for both people with criminal convictions and those who have only been arrested or charged. Across the United States, a strong public policy preference exists for the openness of criminal records, and while each US jurisdiction has a specific set of legislative rules and guidelines regarding the disclosure of criminal records, national cultural and legal norms guide much of state-level decision-making and policy-making. Free speech considerations, open government principles and public safety are routinely invoked to justify the public disclosure of criminal history information (Corda 2016; 2018; Lageson 2017). Criminal records are available to the general public through a vast array of sources, ranging from court records databases and government criminal history repositories to multiple online platforms operating for commercial and non-commercial purposes (Jacobs 2015). In contrast, criminal records databases in Europe are maintained by public authorities and no general principle exists that someone other than those authorities and the record subject is authorized to access a criminal history. Preventing the indiscriminate labelling of individuals with a criminal past as inherently dangerous outcasts has historically been considered instrumental to social reintegration and reducing the likelihood of recidivism (Council of Europe 1984). Despite this overarching framework, however, significant variations in regulating access to and use of criminal records exist across different jurisdictions in the old continent (Loucks et al. 1998; Thomas and Hebenton 2013; Larrauri 2014; Kurtovic and Rovira 2017). In recent years, this has been reinforced by a certain degree of mobility of criminal record policies from the United States to Europe, particularly in regard to vetting policies related to specific offences (Jacobs and Larrauri 2016).

[1] Alessandro Corda, School of Law, Queen's University Belfast, Main Site Tower, University Square, Belfast BT7 1NN, UK; A.Corda@qub.ac.uk; Sarah E. Lageson, Rutgers University–Newark, School of Criminal Justice, 123 Washington Street, Newark, NJ 07102, USA. Both authors contributed equally and are listed alphabetically.

Historically, the rise of criminal record-keeping systems represented a distinctive facet of modern penal strategies guided and informed by ideas of comprehensiveness and coherence (Cole 2001: ch. 1; Corda 2016: 8–15). Since their creation, criminal records have traditionally served two important functions. The first is *informational*—i.e. providing background information on an individual's prior misconduct. The second is *punishment*-related—i.e. connected to the creation of a record codifying a transgression sanctioned by the state. Yet, in today's era of information technology, neither of these functions performs well. If they did, there would be a concerted effort for records to be systematically accurate, evenly accessible and managed by clearly identified and reliable sources. This is not the case. The current state of affairs of criminal records systems resembles more a disorganized, consumer-based digital web of haphazard effects that do not neatly map onto information nor punishment functions. And while the production of criminal records has historically been an internal operation of governmental criminal justice agencies, we argue that private players too are now actively 'producing' criminal records: by extracting, compiling, aggregating and repackaging records from different sources, private companies de facto produce—not merely reproduce— criminal records. The new reality of the creation, release, use and permanence of criminal records thus calls for an adequate understanding and conceptualization of the bureaucratic, social, technological, legal and corporate contexts that produce and reproduce criminal records—a messier and greyer area than other aspects of contemporary criminal justice systems and their ramifications. We refer to this situation as 'disordered punishment'.

The term 'disordered punishment' identifies the largely unpredictable, unevenly imposed, frequently disproportionate and misleading ways criminal records impact people's lives in the digital age. It captures the inconsistent existence of criminal records that do not depend on state action or explicit policies but rather on decisions made by actors located outside the criminal justice system regarding the assembly, dissemination and use of criminal records for various (often market-driven) purposes. 'Disordered punishment' further invokes the difficulties faced by both individuals and governments to manage criminal history information, as it no longer derives primarily from public sources. This marks a significant shift of control over criminal records from government to private interests.

To shed light on this complex phenomenon, we adopt a case study approach. We first conduct an analysis of third-party criminal record disclosure in two cases: the United States, where criminal records are widely available through government and third-party brokers, and Europe, where records are generally legally restricted but increasingly incoherently managed by conflicting players, both public and private. While differences between the United States and Europe regarding criminal record disclosure certainly outnumber the similarities, meaningful experiences in both contexts help illustrate core characteristics of the dynamics of disordered punishment. We thus highlight a not yet fully appreciated pattern of convergence towards the commodification of criminal records perpetuated by corporate actors and leading to chaotic outcomes. Our selected cases are perhaps 'early adopters' of new approaches and technologies, but represent broader emerging trends in criminal record disclosure and dissemination practices. We close with a third case study focusing on the implementation of the 'right to be forgotten' decision in Europe, which has inadvertently transferred powerful control to Google (an American tech company) over the management and visibility of online criminal history information. We use these case studies to develop the framework of 'punishment entrepreneurialism version 2.0', which describes the foundation and context of disordered punishment. Our account combines two influential paradigms in the sociology of punishment presented nearly two decades ago by Feeley (2002) and Jones (2000)—focusing, respectively, on the privatization of state punishment by means of 'penal entrepreneurs' and on the rising role of technology in punishment and control policies and practices, leading to the establishment of a 'digital rule'. We conclude by returning to the dynamics of 'disordered punishment', describing and discussing its characteristics and modes of operation.

Theories, policies and practices of criminal record disclosure

Especially over the past three decades, criminal record management on both sides of the Atlantic has been significantly complicated by information technologies. In the United States, a growing body of scholarship has examined the degree to which the negative consequences of a criminal record are substantially exacerbated with the advent of pervasive background checks, mostly fuelled and made possible by the Internet (Petersilia 2003: 106–112; Lageson 2016; 2017; Lageson and Maruna 2018). In Europe, new technologies have interacted differentially with pre-existing national rules and regulations, revealing in some cases non-negligible gaps. Technological integration of national criminal records databases among EU member countries for cooperation purposes has also not proven immune to loopholes and inadequacies. In both contexts, criminal history information, even if old and expunged from official records, can now easily resurface online even in jurisdictions where criminal records are generally not accessible by non-criminal justice actors. Further, the fight for the right to purge old criminal conviction and arrest information from search results returned by private companies like Google has become a central theme in Europe—but not in the United States—following the acknowledgment of a 'right to be forgotten' online by the European Court of Justice in the so-called Google Spain case (2014).

The public disclosure of criminal convictions is not conceptually part of the legal punishment imposed at sentencing and does not, strictly speaking, serve penal aims such as retribution, deterrence or incapacitation (Lippke 2018). Nonetheless, the publication and dissemination of criminal history information has the ability to considerably enhance and multiply the burdensome ramifications of a conviction (Corda 2016; Hadjimatheou 2016). The disconnection between form and substance as well as between fault and repercussions is even more apparent in the case of non-conviction records. An individual is visibly labelled a 'criminal' even though he or she has never been adjudicated as such (Uggen and Blahnik 2016). Besides amplified social stigma, today's unprecedentedly public criminal records often translate into various forms of discrimination in contexts such as employment (Harding 2003; Pager 2007) and rental housing (Thacher 2008; Kirk 2018).

The legal, sociological and criminological discussion of such forms of criminal record discrimination has largely characterized these effects as informal (or de facto) collateral consequences of run-ins with the law—i.e. neither mandated by operation of law nor imposed at the discretion of a legal authority (Logan 2013; Kirk and Wakefield 2018). Such definition fits with a conceptualization of penality as a field not limited to formal, legal punishment but also encompassing institutions, processes and practices that stem from the penal realm without being formally part of it (Beckett and Murakawa 2012; Kaufman et al. 2018). This way, although not deliberately punitive, criminal records and their consequences can be seen and understood as an integral branch of penal control tactics in risk societies (Logan 2009; Garland 2013: 479; 2017: 4). Whilst in times of penal welfarism excessive stigmatization of ex-offenders and its ramifications were seen as counterproductive and harmful for the profound impact on people's 'self-esteem and prospects of reintegration', especially from the 1990s onwards, 'stigma has become useful again. Doubly useful in fact, since a public stigma can simultaneously punish the offender for his crime and alert the community to his danger' (Garland 2001: 181).

In this article we propose a different theoretical perspective. Rather than conceptualizing the circulation and use of information from criminal records in contemporary society as a penal practice arising from a broad policy preference and approach to public safety and other concurring goals, we posit that the current unprecedented ease of availability and dissemination of criminal records is largely the result of independent technological and bureaucratic shifts that created various appetites for such records. The commodification of criminal records and criminal history information in the digital age has been driven primarily by the intrusion of third parties, which have made criminal background checking a publicized, popularized and almost pop-cultured phenomenon. This intrusion derives from

the desire of companies to attract web-based consumers and to manage and circumvent local bureaucracies and centralized record-keeping. Furthermore, in the old continent, the recent debate on the 'right to be forgotten' adds an additional layer of complexity.

Case 1: The commodification of criminal records in the United States

In the United States, criminal records are widely available through governmental and private sources (Lageson 2016; 2017). Employers and landlords routinely—and legally—access criminal records in making applicant determinations. Civic, educational and voluntary organizations have similarly adopted regular criminal record screening practices. Private criminal background checking companies are regulated through the Fair Credit Reporting Act (FCRA). Operating outside this regulated practice, however, is the vast availability of criminal records on the Internet, accessible at a keystroke to any curious user of the web. The records come from myriad sources: law enforcement agencies and correctional institutions regularly post inmate rosters and booking photos as a public notification service, while courts routinely post a digitized corpus of criminal court records. While long been considered public, these records used to exist only on paper, in practical obscurity (Corda 2016), and were managed by the model has changed dramatically, with data aggregators compiling millions of records to be shared and sold across the web. On the consumer side, this has created a marketplace for websites that range from 'people search engines' to mugshot extortion sites (Stelloh 2017; Lee 2018). These dissemination practices have broad consequences, however, especially in duplicating out-dated and incorrect records (Logan and Ferguson 2016) across web-based platforms.

Public records and people search websites

Because US Freedom of Information laws allow for the release of personally identifiable information, a robust commercial marketplace has emerged that collects, aggregates and repackages public records into a consumer good (Jain 2018). Unlike Europe, where private actors must manipulate or circumvent regulation, American companies can deploy technologies to automatically extract content by 'scraping' or 'crawling' governmental databases or purchase bulk records. These records are then algorithmically matched across identities and sold as pseudo-background check reports. Using these techniques, websites offer what they call 'people search' services, meant to be distinct from official background checks regulated by the FCRA. By arguing that people search websites are simply a web platform performing a search function and not a source of official information, operators claim they are not subject to FCRA regulation.

The FCRA was enacted in 1970 to regulate consumer-reporting agencies (CRAs) by promoting the accuracy, fairness and privacy of information contained in credit reports and background checks. The Act also requires that reporting agencies gather information on the identity of a requester, certify the purpose for running the background check and gain assurance that the record will be used for no other purpose. People search websites, such as *InstantCheckmate.com* and *Pipl.com*, maintain that their companies are based on a wholly different purpose, which is to provide better access to public records. For instance, one company advertises its services in the following terms:

> Instant Checkmate provides you with the most useful, detailed and important information on just about anyone. Whether researching arrest records, phone numbers, addresses, demographic data, census data, or a wide variety of other information, we help thousands of Americans find what they're looking for each and every day.[2]

[2] See https://www.instantcheckmate.com/faqs/.

Individual reports are available for a nominal fee or monthly subscription (about US$20 per report or US$20 per month). These reports contain all public records matched to a particular identity, including birth, marriage and divorce records, email, phone and social media account information, real estate transactions and criminal records obtained from law enforcement agencies and courts that include arrests, charges and digital booking photos. *InstantCheckmate* itself asserts the company 'compiles reports from millions of public records including information provided by state and local governments. All of the information contained in our reports is part of what is referred to as the 'public record''.

To proactively deflect any proposition that they are offering services akin to those offered by a licensed reporting agency, these websites provide disclaimers warning users they are not to use the information for any sort of decision-making (such as hiring or housing decisions) but rather can only use the information for review of public records in an information-gathering spirit. However, the company has no practical oversight over how their customers use the reports in the real world.

Because people search engines operate outside of regulation and depend wholly on local criminal justice agencies to make their records publicly available, the variety, depth and timeliness of disclosed criminal records is unpredictable and contingent upon the geographic locale where the arrest, conviction or incarceration occurred. *InstantCheckmate.com*, e.g., stresses that: 'Each state has different laws regarding public access to these records. Because of this, the criminal records shown on certain reports may be inaccurate or incomplete'. For the record subject, this means their people search report might contain incorrect, out-dated or expunged records. But, because criminal records are now 'owned' by hundreds of sources, the subject can no longer turn to law enforcement or courts for remedy.

Duplication and monetization of public records

Local criminal justice agencies are often left in a quandary for how to cope with the monetization of the records they produce for the public good. This is further complicated when criminal justice agencies, lacking internal technological expertise, contract with private software vendors to maintain internal and public-facing records databases. These software companies help agencies produce data that are replicable and subject to manipulation, such as in the case of Colorado. In the mid-1990s the Colorado court system transitioned to electronic case management and a web-based public access portal. The state hired a data vendor, Background Information Services, that received a copy of the state trial court database, then transferred these data onto the state website. Unbeknownst to the state, however, the company was also transferring the data into a proprietary searchable database, which was later sold to various customers for criminal background check services (Office of the State Court Administrator v. Background Information Services, Inc., 1999).

The state judiciary became aware of these practices only after court staff voiced concerns that inaccurate and confidential personal data were online, including the names of children, sexual assault victims, driver's licenses and social security numbers. The state quickly realized that, '[o]nce vendors received data releases, they were left to their own devices to determine how to program and display the court records' (Colorado Courts 2012: 4). Information was often incomplete, yet records were routinely sold to data brokerage companies across the world. Once the Colorado's court system stopped releasing data to the company, Background Information Services sued for withholding of public data, asking the District Court to order the state to release records again. However, much damage had already been done to the people whose records were duplicated and sold by Background Information Services.

A report by the state notes the difficulties in complying with public access mandates in a digital environment, observing that 'technology limitations and a desire to keep vendors competitive compelled the Department to allow this agent to replicate the data to additional vendors' (Ibid.: 5). By giving a private company access to data, the court system also inadvertently gave private companies

the power to control and disseminate information that could be used to the detriment of people accused, charged and convicted of a crime, moving well beyond the agency's public service intent. These issues were faced by criminal justice agencies across the United States in the 1990s and 2000s. Courts continued to be incentivized to work with private data companies as their digital needs regularly outpaced their technological capacities. At the same time, simply posting court records as an act of public records compliance meant governmental servers were throttled by automated data mining tools that caused websites to crash (Robertson 2011).

The foundational premise for these practices is transparency of public records. In the first scenario discussed above, private actors like *InstantCheckmate.com* compile and repackage existing records into new platforms (not only websites but also smartphone apps), while in the second private actors like Background Information Services directly enter governmental spaces and essentially produce new versions of criminal records for the marketplace. In both scenarios, the creation of a criminal records market means substantial responsibility for criminal labelling falls under the control of private companies, not criminal justice agencies.

Case 2: European loopholes in criminal record management

Compared to the United States, European criminal records are generally less visible and impactful and are widely considered a matter of internal affairs of the justice system (Demleitner 2018: 488). The public availability of information about convictions, not to mention arrests, is deemed to substantially undermine reintegration into society of ex-offenders. However, recent developments in the United Kingdom and Sweden, in particular, offer two notable examples that challenge the oft-praised 'European ethos' in regard to criminal record disclosure policies and practices.

Criminal record forum shopping and UK private vendors

In the United Kingdom, criminal records are regulated by the Rehabilitation of Offenders (ROA) Act of 1974 (Thomas 2007: ch. 5). After a specific period of time has passed (which varies according to the sentence received), certain cautions and convictions automatically become 'spent'. However, growing public desire to access records has created two controversial practices: first, employers have begun to ask applicants to supply their own records when they are unavailable from the government. Further, private companies have begun to access UK residents' records, exploiting legal and technological loopholes and building businesses around this practice.

There are three levels of criminal background checks administered by the Disclosure and Barring Service (a non-departmental public body of the UK Home Office): Basic, Standard and Enhanced, which outline various levels of disclosed record information based on the type of job a person is applying for (Henley 2018: 287–290). Although the ROA limited access, penal discourse and policies began to reject rehabilitation in the late 1970s culminating in 'law and order' political imperatives in the 1980s and populist and punitive rhetoric in the early 1990s (Newburn 2007; Loader 2006). Over time, a false expectation amongst employers, landlords, insurers, etc. that they are required to run a background check and ask about 'unspent' convictions and cautions, even when no such obligation exists.

The new discourse around crime (Garland 2001) also triggered a certain degree of impatience. A growing number of professional and voluntary organizations vigorously lobbied the government to be included in the list of 'exempted' occupations and sectors for which standard and enhanced checks, revealing both spent and unspent criminal history information, can be requested, significantly eroding the rule (Marshall and Thomas 2017: 240). Employers excluded from these exemption lists succeeded in bypassing regulation by requesting prospective employees or volunteers to provide, as part of their

application, a copy of their own 'police check'—a document issued by the Police at the request of the concerned individual disclosing data stored on the Police National Computer (PNC) about them, including spent and unspent convictions and cautions, plus arrests that did not result in any prosecution. This widespread practice, known as 'enforced subject access', was not only inherently against the spirit of the data protection regulation (police check information is provided only for personal use and no one else has a right to ask for such information) but nullified the ROA goal of providing a second chance.

In 2014, Section 56 of the Data Protection Act 1998 (now Section 184 of the Data Protection Act 2018) halted these 'back-door' criminal record checks by criminalizing a request to an individual to exercise their subject access rights to access to their criminal history and provide it to another person (Information Commissioner's Office 2015). Yet, shortly after the criminalization of enforced subject access, a number of websites appeared that promised to provide criminal histories otherwise inaccessible under national law. Target customers are private citizens, employers or organizations that want to satisfy a craving to know more than they are legally allowed to. The following comes from the website of one the main companies offering such services to customers online:

> Up to now you had to strike a balance between a desired depth of the criminal history check and the channels you were legally eligible for. Luckily, you do not need to compromise anymore, as....
>
> THERE IS AN ALTERNATIVE!
>
> Thanks to the European Union directive on exchange of criminal records among EU member states, UK criminal records are now accessible through other EU member states' criminal record bureaus.
>
> The process is simple and does not infringe the UK laws.
>
> As specialists in European Union criminal record checks, we have created a process that allows you to perform such checks on individuals in various EU member states, including United Kingdom. Simply send us a written application form completed by the subject and a scan or a digital picture of his/her ID. You do not need to register with umbrella bodies or follow timely procedures. Just complete the order form. We take it from there![3]

This company—which, interestingly enough, uses the same acronym of the official EU system—is based and operates in the United Kingdom but obtains criminal record certificates via the Polish National Criminal Register, which has access to the criminal record databases of most EU member states through the European Criminal Records Information Exchange System (ECRIS). ECRIS established electronic interconnections between EU countries in 2012 and standardized electronic formats so that records could be shared amidst government actors across countries in a uniform and speedy way. Just like the FBI's Interstate Identification Index system (so-called 'Triple I') in the United States, the ECRIS system is based on a decentralized architecture where criminal records data are stored solely in national databases and are exchanged electronically upon request (Plachta 2007; Roux-Demare 2012). This company exploits the ECRIS regulation by filing a request in Poland, accompanied by the written authorization of the concerned subject (e.g. the job applicant or applicant for a tenancy agreement).[4]

This is possible since enforced subject access is not currently outlawed in that country. The certificate, generally in a standardized ECRIS template, is then issued in Polish and transmitted to the

[3] See http://ecris.eu/criminal-record-uk/.

[4] The company lists 'applicants' awareness and consent' as core values, underscoring that 'we do not involve in any activities
carried out without subject's knowledge' (see http://ecris.eu/eu-criminal-record-check/).

customer alongside an English translation. The average turnaround time is four business days and the price for the service is £79 (around US$100). Most importantly, this certificate provides information on both spent *and* unspent convictions, in addition to possible disqualifications arising from them. Furthermore, such information is not subject to any filtering mechanism now in place under UK law.[5] The service provided by websites of this kind therefore enables UK individuals and organizations that are not entitled to obtain anything more than information contained in a basic check to (potentially) get much more information.

Such 'criminal record forum shopping' is made possible by the sharing of criminal history information between countries with different legislations, frustrating the main goal of the ROA 1974 and circumventing the prohibition on enforced subject access passed in 2014 by making the implementation of a 'transnational enforced subject access' possible. Because the conduct is committed outside the United Kingdom, there is no UK jurisdiction to prosecute. This is an illustrative example of how technological development, integration and information sharing at the EU level and the use of the Internet as a powerful commercial tool have enabled and incentivized for-profit private players to develop workaround tactics. These actors take advantage of decentralized access to national criminal record databases to sell criminal record information that could not be otherwise lawfully obtained domestically. In the described example, Polish legislation provides an ideal back-door entry to gain access to criminal record information that is normally not subject to disclosure in the United Kingdom.

Rather ironically, the establishment of the ECRIS system was primarily envisaged to allow authorities of EU member states to prevent people with convictions travelling across borders from escaping their criminal past in a different country. Now, private vendors travel to foreign jurisdictions with different regulations but with access to much of the same data to collect criminal history information whose disclosure and use have been banned at home.

Scandinavian outlier: the case of Swedish private criminal record databases

In spite of long-standing traditions of transparency and open government (Rosengren 2017: 77–78), Sweden has historically treated criminal records differently from other public records. The centralized National Criminal Records Registry was created in 1901 with the goal of preventing leaks from local repositories and enabling the government to maintain full control over the management of criminal history information. For nearly a century, only state authorities and listed public employers (e.g. airports, mental health services, children and youth care facilities) had access to the criminal records registry (Backman 2012a). This exception to the general rule of unrestricted access to official records was justified not only as a crucial means to contrast recidivism and favour social reintegration but also as 'an important strategy in managing the perceived risks' potentially posed by individuals with a criminal record (Backman 2011: 111). To prevent the spread of enforced subject access, individuals were even denied access to their own criminal history record until 1989. Only in the early 2000s, the

[5] The case R (T and others) v Chief Constable of Greater Manchester Police and others (2013) established that the automatic disclosure of all spent and unspent convictions and cautions in standard and enhanced checks is disproportionate and, therefore, incompatible with the right to private life under Article 8 of the UK Human Rights Act. After initial resistance, the Government responded by introducing a 'filtering system', which identifies under what conditions old and minor convictions and cautions can no longer be disclosed in standard and enhanced checks. In 2019, the UK Supreme Court considered the compatibility of the amended legislative regime and recognized the disproportionality of the blanket rules requiring the automatic disclosure of all convictions for individuals with more than one prior conviction on record and the requirement that some juvenile cautions be disclosed indefinitely (R (P, G and W) and R (P) v Secretary of State for the Home Department and others 2019).

list of employers allowed or obliged to perform a background check on applicants and employees was considerably broadened (Backman 2012b).

However, in 2014, exposure of people with a criminal record reached an unprecedented level within the European borders when the website *Lexbase.se* was launched, releasing information about all criminal convictions imposed in Sweden since 2009 upon the payment of a small fee (around US$10 per request). The *Lexbase* database became immediately popular. Users could search for a specific name, street or ID number or view a map with red dots at the addresses where people with a record reside. The service also alerted users when they walk into a neighbourhood with a high proportion of residents with a criminal past (The Economist 2014).

Lexbase capitalized on pre-existing rules to accessing public records that were not prepared for the digital age. While criminal records were kept private, local court records were made available for a period of six years following the issuance of the final verdict in criminal cases. This meant that, at least in theory, the general public already had the option of retrieving criminal convictions from the courts. But as long as court records were locally stored and not available in an electronic form, it was extremely laborious to retrieve information on specific individuals. In recent decades, however, case files have been digitized and indexed in electronic databases, made accessible in each district and appeal court via a public computer terminal. People were able to search local court records and then ask a clerk for a copy of a specific verdict. More recently, a user-friendlier model was developed allowing citizens to call or email a given court and ask if they had anything on a certain person and, if so, have such records sent as a PDF file.

What *Lexbase* did was simply ask Sweden's 48 local district courts to release digitized decisions in criminal cases upon the payment of an administrative processing fee. After obtaining bulk information, they created a single searchable database available to the general public. It must be noted that a number of similar databases were already accessible online but were not designed for a general audience; rather, criminal history information had been made available to selected customers such as journalists, certain employers, lawyers and universities at very high service fees. Lexbase.se thus unhinged the pre-existing status quo characterized by an overall limited access to the national criminal record database while being in full compliance with existing rules.

This was essentially a clever use of constitutional rights, pre-existing protections for the media, and use of new technologies to meet and stimulate the growing appetite of the general public for criminal history information.[6] The Swedish Department of Justice could not successfully press charges against the owners of the website since no violation had been committed. *Lexbase.se* was, and still is, operating in full compliance with the law, having been regularly granted a so-called publication license issued by the Swedish Press and Broadcasting Authority. Such a license, primarily aimed at promoting freedom of information and expression, protects publishers and public records information databases, largely insulating them from any possible criminal and civil liability.[7]

A heated debate has followed, with many parties calling for an amendment to the Fundamental Law on Freedom of Expression to limit the ability of websites like Lexbase.se to exploit public access principles and statutes for commercial purposes (The Local 2014a).[8] Attempts to curb this model have failed due to an effective campaign prompted by private vendors and embraced by conservative circles

[6] Information gathered from official records is gradually extending to include decisions not to prosecute made despite substantial evidence of guilt (Svenska Dagbladet 2016).

[7] The publication license is valid for 10 years and can then be renewed. The requirements to obtain or renew such license are currently rather formalistic.

[8] The government suggested restricting access to *Lexbase* to legal professionals and government-approved journalists. The rationale offered is that criminal history information made indiscriminately available infringes on the person's individual integrity in a more serious way than information obtained through pre-existing services targeting specific audiences and more limited in scope.

suggesting that amendments to existing rules may introduce limitations to the free flow of information and promote undue government oversight on the media.

In 2014, a spokesperson for Lexbase.se stated that 'the service was in line with the times and suits Swedes' desire for information. …The underlying idea [in Swedish legislation] is that transparency is a good thing. We are just making it more modern'. Another point made was that 'the website—for example—could help women on the dating scene, as they might want to know if their prospective date had any previous convicts for rape or assault' (The Local 2014b). This statement captures key factors in the gradual normalization of a background checking culture in Sweden. Lexbase and other criminal record databases subsequently established have largely succeeded in developing a reassuring narrative: they are simply offering the general public an important service that certain professionals have been able to access for more than two decades through other databases. Criminal records purveyors have thus appealed directly to core values of the Swedish state, community and general political culture such as democratic egalitarianism, openness and transparency to depict their business not only as unproblematic and legitimate but also as fully consistent with the country's ethos.

Similarly, the modernization argument has been used to downplay the negative aspects of criminal record disclosure by suggesting an alleged continuity with long-established values now merely presented in an updated version, where principles of open government meet digital technology. This 'selling proposition' is further reinforced by the awareness of how technology can improve 'better safe than sorry' techniques. Finally, function creep in the management of accessible criminal record repositories and the creation of private commercial databases have disrupted the distinction, originally envisioned by the government, between public records 'for the public good' and public records carrying individual stigma.

Case 3: Right to be forgotten online and the expansive role of Google in criminal history information management

In 2014, the ruling issued by the Grand Chamber of the Court of Justice of the European Union in the Google Spain case (2014) allowed private citizens of European countries to request search engines to delist information about themselves from search results, acknowledging a 'right to be forgotten' (RTBF) online (Stacey 2017). The criteria articulated in the *Google Spain* judgment have been substantially codified in Article 17 of the 2018 EU General Data Protection Regulation (GDPR). In deciding what to delist, search engines like Google must consider if the information in question is inaccurate, inadequate, irrelevant or excessive and whether there is a public interest in the information remaining available in search results. Since the judgement was issued, Google received nearly 1 million requests to delist over 2.5 million URLs. In the case of news, requests most frequently targeted articles covering crime (22.8 per cent) (Bertram et al. 2018).

Google has taken a rather active approach in the delisting process regarding criminal history information. Google's Transparency Report states that company staff make initial decisions about requests to delist (Google, Inc. 2018). If Google decides not to remove a certain URL from search results, an individual may request that his or her national Data Protection Authority review the decision. Past this stage, an appeal may be filed before a national judge. When it comes to delisting information pertaining to criminal records specifically ('spent [sealed/expunged] convictions/exonerations/acquittals for crimes'), in its guidelines Google states the following:

> Consistent with local law governing the rehabilitation of offenders, we tend to weigh in favor of delisting content relating to a conviction that is spent, accusations that are proved false in a court of law or content relating to a criminal charge of which the requester was acquitted. We also consider the age of this content and the nature of the crime in our analysis. (emphasis added).

The statement notes that factors weighing a decision not to delist a page include whether there is a 'strong public interest' in the information it contains, such as a person's past crimes and positions in public life. These guidelines thus suggest that Google is willing to interpret, tweak and ultimately challenge policy and legislative determinations made at the national level regarding the management of criminal records of people who have been deemed legally rehabilitated. Simply, the company assesses whether it is in the public interest to remove a link to criminal history information that, under national law, should be squarely forgotten. These unilaterally heightened margins of discretion are apparent in some of the cases that Google itself presents as examples in its Transparency Report:

> UNITED KINGDOM: We received a request to delist news articles from more than 10 years ago about a woman who killed her abusive husband and then attempted suicide. We initially pushed back on the request but the Data Protection Authority asked that we delist, as her sentence is spent under UK law *and she did not appear to be a threat to others*. We eventually delisted 3 news articles about the incident (emphasis added).
>
> GERMANY: A teacher convicted for a minor crime over 10 years ago asked us to remove an article about the conviction. We have removed the pages from search results for the individual's name.
>
> HUNGARY: A high-ranking public official asked us to remove recent articles discussing a decades-old criminal conviction. We did not remove the articles from search results.

In the UK example, the company agrees to delist on the basis that the person does no longer 'appear to be a threat to others'—a criterion that is nowhere to be found in both legislation and case law. In the German and Hungarian examples, Google reaches different conclusions based on its autonomous judgement; newspaper articles discussing an older conviction do not deserve to be delisted if they concern a person involved in public life. A more recent conviction, in turn, can be delisted if it concerns a minor offence committed by an individual with no public roles. Once again, neither the legislature nor courts have articulated any such criteria.

The management of the RTBF by a powerful private player like Google raises important questions not only about the privatization of privacy but also the privatization of inflicting punitive effects via the online availability of criminal history information. Google is taking on a role previously performed by the state—i.e. deciding which records (or, better, proxies for records) are public or not, seemingly applying criteria it has, at least partially, determined on its own. That a powerful private player like Google has become so dominant that it can even 'usurp' or, at least, influence state functions (Powles and Chaparro 2015) illustrates how the privatization of punishment is now also regulated via the privatization of privacy.

A recent UK High Court case (NT1 & NT2 v Google LLC 2018) shows this in action. The case involved the decision of whether two businessmen, NT1 and NT2, had the right to have links concerning past convictions, now deemed spent under the ROA 1974, removed from search results. They sued Google for breach of privacy rights and the misuse of private information following the company's refusal to delist a number of URLs, including various links to national newspaper articles. NT1 was convicted for conspiracy to account falsely and sentenced to four years' imprisonment after

trial. NT2 was convicted for conspiracy to carry out surveillance and sentenced to six months' imprisonment in a guilty plea. Despite both convictions being deemed spent under UK law and, therefore, to be treated as if they never happened, the court ruled in favour of NT2 but against NT1 claiming substantial differences between the two situations. The court notes that NT2 has sincerely 'acknowledged his guilt, and expressed genuine remorse'. Furthermore, the court notes, 'no evidence' exists 'of any risk of repetition [as] [h]is current business activities are in a field quite different from that in which he was operating at the time' (para. 223). In contrast, the court observes that, regardless of any legal determination, the information about the spent conviction of NT1 'retains sufficient

relevance today' since the concerned individual 'has not accepted his guilt, has misled the public…and shows no remorse'.

The judgment also notes that NT1 is still in the same business and, therefore, the online accessibility of the information serves 'the purpose of minimising the risk that he will continue to mislead, as he has in the past' (para. 170).[9] The judgment was presented in the media as a 'landmark' defeat for Google in a RTBF online case (Grierson and Quinn 2018). But is this accurate? The court seems to accept and even mimic Google's approach to re-assess convictions that have already been deemed spent/sealed under national law. Although the court recognises that a conviction being spent will normally be a weighty factor against the further use or disclosure of information, it does take into account post-release behaviour, current occupation and perceived level of 'riskiness' of the concerned subjects to reach divergent conclusions in the two cases considered. This is highly problematic from a penal policy standpoint. A private sector-led, case-by-case re-litigation of record sealing policies for those individuals deemed rehabilitated by law might crucially undermine the credibility and effectiveness of second chance relief mechanisms. In the digital age, just like zombies, 'dead' criminal records can come back to inflict significant harm, even after they have reached the end of their 'natural' legal life.

Punishment entrepreneurialism 2.0

Our analysis illustrates the rapidly changing character of criminal record production and disclosure in different regulatory contexts. The openness of records in the United States has allowed for greater monetization and commodification of such records than seen in Europe. But while the scale and legalities of access may differ, emerging practices in both contexts do bear important similarities. The capture of records without explicit consent or knowledge of the originating governmental agency and the exponential growth of loosely regulated websites and other digital platforms that exploit these records for commercial purposes represent a clear pattern of convergence. In this section, we develop the account of what we term 'punishment entrepreneurialism version 2.0', which describes today's reality of criminal record disclosure and management dominated by private, for-profit companies. Two influential accounts presented in the early 2000s separately addressed the issues of privatization and the emerging role of technology in punishment policies and practices. Combined together, they represent the version 1.0 of privatization of punishment in a context of technological development. The version 2.0 we present here does not supersede but rather complements the 1.0 version.

In Feeley's (2002) account of penal entrepreneurs, private players collaborate with the government to dispense and implement state-imposed punishment—i.e. punishment imposed at the sentencing stage of the criminal justice process. Private prisons and privatization of probation services are paradigmatic examples. First generation penal entrepreneurs follow a *contractual* model for they exercise forms of delegated authority as contractors of the state. A formalized public–private partnership is thus essential to perform criminal justice functions. Penal entrepreneurs version 1.0 are legitimized in what they do since they are formally entrusted with taking over traditional penal institutions such as prisons and community corrections, and incentivized to innovate in order to expand or maximize profit. In the context of penal entrepreneurialism version 1.0, the role of technology translates into a concentrated form of 'digital rule' described by Jones (2000). The government decides to adopt a newly available technology but authorizes private players to deploy it to carry out a governmental function such as in the case of electronic monitoring and location tracking by private community supervision providers. Regardless of the source of innovation (the state or penal entrepreneurs themselves), the use of technology and its effects in the penal sphere are the outcomes

[9] NT1's appeal against the decision was eventually withdrawn. However, it has not been disclosed whether eventually Google accepted to delist the links in question or NT1 decided not to proceed further.

of a deliberate policy choice centrally made at the government level that expands or innovates traditional forms of punishment and control mechanisms.

As summarized in Table 1, in the context of what we refer to as 'penal entrepreneurialism 2.0', both these aspects significantly change. First, while the 1.0 version is mostly concerned with functions of state punishment outsourced to private actors, second generation penal entrepreneurs break the delegated, contractual mode typical of the original paradigm of involvement of private, for-profit actors. Rather, they follow an opportunistic mode of action operating under no authority from the state. Private data vendors accessing, mining and commodifying digital criminal records and web search engines exercising significant discretion about what criminal history information should be available or not both represent quintessential examples of this new version of the privatization of punishment. No formalized public–private partnership exists anymore. Private players do not privatize segments of the criminal justice system in the traditional understanding of the term. They are not, in other words, agents of the state. Rather, private actors circumvent, manipulate or resist government and judicial regulation in the criminal records market. Under this scenario, the described disorderly amplification of the reach of the penal state does not result from a concerted effort. New penal entrepreneurs, instead, perform a function that is conceptually and operationally detached and distinct from state-imposed punishment and control strategies.

With regard to the use of technology, unlike the 1.0 concentrated version, the 2.0 version of penal entrepreneurialism is characterized by a dispersed form of 'digital rule'. This means that no concentrated rule exerted by a single ruler (i.e. the government) exists anymore. An ever-increasing number of private companies access, compile, repackage and sell criminal records online for commercial purposes; Internet players actively disclose and make determinations concerning criminal history information representing 'proxies' for criminal records online (news coverage of a certain event, crime watch blog posts, etc.), oftentimes frustrating the effectiveness of relief mechanisms. Technology has formidably facilitated the exploitation of criminal record data, favouring the aggregation of numerous bits of information that are then sold or variously disclosed and managed, frequently in violation of the spirit of transparency and privacy laws and policy, which, for the time being, have shown their obsolescence and inadequacy for the digital age. This has serious consequences for the subjects of criminal records who increasingly find themselves the target of 'disordered punishment'.

TABLE 1 *The two generations of punishment entrepreneurialism*

	Penal entrepreneurs	Role of technology
Punishment entrepreneurialism version 1.0	Formalised public-private partnership Penal entrepreneurs are contractors of the state and operate within set boundaries Penal entrepreneurs administer outsourced state-imposed punishment (e.g., private prisons and probation services)	Concentrated form of 'digital rule' exercised by the government Technology expands traditional punishment and control mechanisms (e.g., electronic monitoring in community supervision)
Punishment entrepreneurialism version 2.0	No public-private partnership exists Penal entrepreneurs autonomously collect and commodify criminal records data, and exert discretion on disclosure Penal entrepreneurs perform a function that is conceptually and operationally detached and distinct from state punishment and control strategies	Dispersed form of 'digital rule' exercised by private actors Various private actors exploit technological developments to access, compile, sell, disseminate, and manage criminal history data

The advent of disordered punishment

These shifts profoundly affect the experience of contemporary punishment for individuals with a criminal record. In the current age, intrinsically linked to digital services and products, private companies take advantage of loopholes to work around regulations and have now become the dominant player in this area of the criminal justice landscape thanks to their ability to compile and organize large criminal record databases from multiple sources. Private companies, helped and boosted by technological developments, transform government data into a valuable commodity fuelling a fear-based consumerism. The myriad of websites and apps claiming to ensure fast and accurate criminal background checks perfectly epitomize it. At the same time, they import tech logic into the realm of punishment, with its allure of being objective, transparent and efficient. Yet there is nothing systematic, efficient or invariably predictable in regard to both the level of utilization and outcomes of today's criminal record checks. Rather, in an almost completely unplanned fashion, something new has emerged, prompted by technological developments and a substantial shift in the narrative around crime at the societal level. This calls into question some of the features that have been identified as distinctive of the current penal era. In the context of criminal record disclosure and management practices, we are not dealing with strategies implemented by state or state-delegated actors 'pursu[ing] systemic rationality and efficiency' (Feeley and Simon 1992: 452). Quite the contrary, the compilation,

disclosure, dissemination and use of criminal records have come to represent what we term 'disordered punishment'.

Disordered punishment is generated inconsistently across multiple, overlapping platforms and increasingly difficult for both government and individuals to manage. It is characterized by a shift of control of criminal record information from government to private interests, which in turn shapes the form, content and reach of criminal records. This shift in control cannot be understated as it tilts power into the hands of an unregulated or underregulated private sector, subverting deep-seated principles of justice. Technological developments simultaneously fuel the appetite for information and stimulate new players to get into the market of criminal justice information, playing a fundamental role in triggering the disordered punishment phenomenon. In the context of this mutually reinforcing interconnection, customers of background checking companies—and, more generally, users of criminal records information propagated by technological innovation—actively participate in chaotically enhancing the propagation of punitive effects beyond formally imposed punishment.

The exponentially increased accessibility of criminal records is at odds with both retributive and consequentialist penal aims (Corda 2016: 42–46). Even more fundamentally, the spread of records via technology and third parties has in many ways outpaced and disrupted the original, theoretical intent of criminal record policy. Key and traditionally desired features of state-imposed punitive reactions such as certainty, uniformity, proportionality and the ability to clearly communicate with the offender and society at large (Duff 2001; Tonry 2011) are substantially undermined. In particular, the lives by making punishment disordered by way of the oft-overlapping qualities of being:

(1) Unpredictable.
(2) Unevenly imposed.
(3) Disproportionate.
(4) Misleading.

The quality of being unpredictable depends primarily on the fact that, in a significant number of instances, the law does not mandate criminal background checks. Therefore, individual sensibilities and attitudes towards vetting play a key role. Whether a background check is conducted largely rests in the hands of private decision-makers whose risk perception and risk aversion may vary substantially. And even if such checks are performed, there is still the possibility of both false positives and false negatives since databases are not always complete, accurate or up to date and often report mismatched identities. Employers, insurers and landlords—but also neighbours, acquaintances and potential partners—ultimately determine whether impactful consequences are imposed and, if so, with what magnitude. Laypersons generally lack specific knowledge or expertise to make informed forward-looking determinations based on someone's criminal past, which significantly increases the chance of an uneven and inconsistent imposition of such consequences. The consequences of having a criminal record are also often disproportionate in their impact. Background checking conducted via multiple channels indiscriminately affects people with a prior encounter with the criminal justice system, regardless of the seriousness of the offence or the outcome of the police's initial action. Finally, disordered punishment can be misleading as background checking conducted via a vast array of available private platforms, widely accessible online, frequently provides information that is not always easily intelligible. The ability to interpret someone else's criminal record correctly can ultimately determine the impact such record will have.

References

Backman, C. (2011), 'Regulating Privacy: Vocabularies of Motive in Legislating Right of Access to Criminal Records in Sweden', in S. Gutwirth, Y. Poullet, P. De Hert and R. Leenes, eds., Computers, Privacy and Data Protection: An Element of Choice. 111–37. Springer.

—— (2012a), 'Criminal Records: Governing Symbols', in B. Larsson, M. Letell and H. Thörn, eds., Transformations of the Swedish Welfare State: From Social Engineering to Governance? 120–34, Palgrave Macmillan.

—— (2012b), 'Mandatory Criminal Records Checks in Sweden: Scandals and Function Creep', Surveillance & Society, 10: 276–91.

Beckett, K. and Murakawa, N. (2012), Mapping the Shadow Carceral State: Toward an Institutionally Capacious Approach to Punishment', Theoretical Criminology, 16: 221–44.

Bertram, T., Bursztein, E., Caro, S., Chao, H., Feman, R. C., Fleischer, P., Gustafsson, A., Hemerly, J., Hibbert, C., Invernizzi, L., Donnelly, L. K., Ketover, J., Laefer, J., Nicholas, P., Niu, Y., Obhi, H., Price, D., Strait, A., Thomas, K. and Verney, A. (2018), 'Three Years of the Right to be Forgotten', Google, Inc., 1–17.

Cole, S. A. (2001), Suspect Identities: A History of Fingerprinting and Criminal Identification. Harvard University Press.

Colorado Courts (2012), 'Data Replication Report: Task Force Recommendations to the Public Access Committee', available online at https://www.courts.state.co.us/userfiles/file/Administration/JBITS/Court_Services/Public%20Access%20Advisory%20Committee/Data%20Replication%20Task%20Force%20Report%202012.pdf (accessed 23 December 2018).

Corda, A. (2016), 'More Justice and Less Harm: Reinventing Access to Criminal History Records', Howard Law Journal, 60: 1–60.

—— (2018), 'Beyond Totem and Taboo: Toward a Narrowing of American Criminal Record Exceptionalism', Federal Sentencing Reporter, 30: 241–51.

Council of Europe (1984), The Criminal Record and Rehabilitation of Convicted Persons. CoE Publications Section.

Demleitner, N. V. (2018), 'Collateral Sanctions and American Exceptionalism: A Comparative Perspective', in K. R. Reitz, ed., American Exceptionalism in Crime and Punishment. 487–525. Oxford University Press.

Duff, R. A. (2001), Punishment, Communication, and Community. Oxford University Press.

Feeley, M. M. (2002), 'Entrepreneurs of Punishment: The Legacy of Privatization', Punishment & Society, 4: 321–44.

Feeley, M. M. and Simon, J. (1992), 'The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications', Criminology, 30: 449–74.

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

—— (2013), 'Penality and the Penal State', Criminology, 51: 475–517.

—— (2017), 'Penal Power in America: Forms, Functions and Foundations', Journal of the British Academy, 5: 1–35.

Google, Inc (2018), 'Transparency Report: Search Removals under European Privacy Law', available online at https://transparencyreport.google.com/eu-privacy/overview (accessed 23 December 2018).

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12. Court of Justice of the European Union (Grand Chamber), 13 May 2014.

Grierson, J. and Quinn, B. (2018), 'Google Loses Landmark 'Right to be Forgotten' Case', The Guardian, 13 April 2018, available online at https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case (accessed 23 December 2018).

Hadjimatheou, K. (2016), 'Criminal Labelling, Publicity, and Punishment', Law and Philosophy, 35: 567–93.

Harding, D. J. (2003), 'Jean Valjean's Dilemma: The Management of Ex-convict Identity in the Search for Employment', Deviant Behavior, 24: 571–95.

Henley, A. J. (2018), 'Mind the Gap: Sentencing, Rehabilitation and Civic Purgatory', Probation Journal, 65: 285–301.

Information Commissioner's Office (2015), 'Law Change Outlaws 'Back Door' Criminal Record Check', available online at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/03/law-change-outlaws-back-door-criminal-record-check/ (accessed 23 December 2018).

Jacobs, J. B. (2015), The Eternal Criminal Record. Harvard University Press.

Jacobs, J. B. and Larrauri, E. (2016), 'European Criminal Records and Ex-Offender Employment', Oxford Handbooks Online, available online at http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199935383.001.0001/oxfordhb9780199935383-e-157 (accessed 23 December 2018).

Jain, E. (2018), 'Capitalizing on Criminal Justice', Duke Law Journal, 67: 1381–431.

Jones, R. (2000), 'Digital Rule: Punishment, Control and Technology', Punishment & Society, 2: 5–22.

Kaufman, N., Kaiser, J. and Rumpf, C. (2018), 'Beyond Punishment: The Penal State's Interventionist, Covert, and Negligent Modalities of Control', Law & Social Inquiry, 43: 468–95.

Kirk, D. S. (2018), 'The Collateral Consequences of Incarceration for Housing', in B. M. Huebner and N. A. Frost, eds., Handbook on the Consequences of Sentencing and Punishment Decisions. 53–68. Routledge.

Kirk, D. S. and Wakefield, S. (2018), 'Collateral Consequences of Punishment: A Critical Review and Path Forward', Annual Review of Criminology, 1: 171–94.

Kurtovic, E. and Rovira, M. (2017), 'Contrast between Spain and the Netherlands in the Hidden Obstacles to Re-entry into the Labour Market Due to a Criminal Record', European Journal of Criminology, 14: 502–21.

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

—— (2017), ‘Crime Data, the Internet, and Free Speech: An Evolving Legal Consciousness’, Law & Society Review, 51: 8–41.

Lageson, S. E. and Maruna, S. (2018), ‘Digital Degradation: Stigma Management in the Internet Age’, Punishment & Society, 20: 113–33.

Larrauri, E. (2014), ‘Legal Protections against Criminal Background Checks in Europe’, Punishment & Society, 16: 50–73.

Lee, E. (2018), ‘Monetizing Shame: Mugshots, Privacy, and the Right to Access’, Rutgers University Law Review, 70: 557–645.

Lippke, R. (2018), ‘Legal Punishment and the Public Identification of Offenders’, Res Publica, 24: 199–216.

Loader, I. (2006), ‘Fall of the ‘Platonic Guardians’: Liberalism, Criminology and Political Responses to Crime in England and Wales’, British Journal of Criminology, 46: 561–86.

Logan, W. A. (2009), Knowledge as Power: Criminal Registration and Community Notification Laws in America. Stanford University Press.

—— (2013), ‘Informal Collateral Consequences’, Washington Law Review, 88: 1103–17. Logan, W. A. and Ferguson, A. G. (2016), ‘Policing Criminal Justice Data’, Minnesota Law Review, 101: 541–616.

Loucks, N., Lyner, O. and Sullivan, T. (1998), ‘The Employment of People with Criminal Records in the European Union’, European Journal on Criminal Policy and Research, 6: 195–210.

Marshall, D. and Thomas, T. (2017), Privacy and Criminal Justice. Palgrave Macmillan. Newburn, T. (2007), ‘“Tough on Crime”: Penal Policy in England and Wales’, Crime and Justice: A Review of Research, 36: 425–70.

NT1 & NT2 v Google LLC [2018] EWHC 799 (QB).

Office of the State Court Administrator v. Background Information Services, Inc., 994 P.2d 420 No. 99SC381 (Colo. 1999).

Pager, D. (2007), Marked: Race, Crime, and Finding Work in an Era of Mass Incarceration. University of Chicago Press.

Petersilia, J. (2003), When Prisoners Come Home: Parole and Prisoner Reentry. Oxford University Press.

Plachta, M. (2007), ‘Criminal Records in an Era of Globalization: Identifying Problems and Conceptualizing Solutions within the European Union’, International Criminal Law Review, 7: 425–47.

Powles, J., and Chaparro, E. (2015), ‘How Google Determined Our Right to be Forgotten”, The Guardian, 18 February 2015, available online at https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search (accessed 23 December 2018).

R (P, G and W) and R (P) v Secretary of State for the Home Department and others [2019] UKSC 3.

R (T and others) v Chief Constable of Greater Manchester Police and others [2013] EWCA Civ 25.

Robertson, J. (2011), 'When Your Criminal Record Isn't Yours, Associated Press, 16 December 2011, available online at https://www.deseretnews.com/article/700207627/AP-IMPACTWhen-your-criminal-past-isnt-yours.html (accessed 23 December 2018).

Rosengren, A. (2017), 'The Swedish Black Box: On the Principle of Public Access to Official Documents in Sweden', in P. Jonason and A. Rosengren, eds., The Right of Access to Information and the Right to Privacy: A Democratic Balancing Act. 77–109. Södertörn University.

Roux-Demare, F. X. (2012), 'Towards the Creation of a European Criminal Record', Revue Internationale de Droit Comparé, 64: 777–91.

Stacey, C. (2017), 'Rehabilitation in the Internet Age: The Google-effect and the Disclosure of Criminal Records', Probation Journal, 64: 269–75.

Stelloh, T. (2017), 'Innocent Until Your Mug Shot Is on the Internet', The New York Times, 4 June 2017, SR10.

Svenska Dagbladet (2016), 'Kritiserade Lexbase bygger ut', 2 February 2016, available online at https://www.svd.se/kritiserade-lexbase-bygger-ut (accessed 23 December 2018).

Thacher, D. (2008), 'The Rise of Criminal Background Screening in Rental Housing', Law & Social Inquiry, 33: 5–30.

The Economist (2014), 'Privacy Rights v Rights to Access Information: A New Website Lets Swedes Check Their Neighbours' Criminal Records', 29 January 2014, available online at https://www.economist.com/charlemagne/2014/01/29/privacy-rights-v-rights-to-accessinformation (accessed 23 December 2018).

The Local (2014a), 'Crime Record Site Shows Sweden's Constitution Needs to Be Rewritten', 28 January 2014, available online at https://www.thelocal.se/20140128/crime-record-siteshows-constitution-needs-to-be-rewritten (accessed 23 December 2018).

—— (2014b), 'Site Lets Swedes Snoop on Friends' Criminal Past', 27 January 2014, available online at https://www.thelocal.se/20140127/track-a-criminal-app-to-launch-in-sweden (accessed 23 December 2018).

Thomas, T. (2007), Criminal Records: A Database for the Criminal Justice System and Beyond. Palgrave Macmillan.

Thomas, T. and Hebenton, B. (2013), 'Dilemmas and Consequences of Prior Criminal Record: A Criminological Perspective from England and Wales', Criminal Justice Studies, 26: 228–42.

Tonry, M. (2011), 'Punishment', in M. Tonry, ed., The Oxford Handbook of Crime and Criminal Justice. 95–125. Oxford University Press.

Uggen, C. and Blahnik, L. (2016), 'The Increasing Stickiness of Public Labels', in J. Shapland, S. Farrall and A. Bottoms, eds., Global Perspectives on Desistance: Reviewing What We Know and Looking to the Future. 222–43. Routledge.

The published version is available at the following link: https://doi.org/10.1093/bjc/azz039