Anil Kalhan
Professor of Law, Drexel University

Written Submission for UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance
Expert Workshop on Race, Borders, And Digital Technologies, June 16-17, 2020[1]

Like other areas of contemporary governance, immigration control has rapidly become an information-centered and technology-driven enterprise. At every stage of the process of migrating or traveling to, from, and within the United States, individuals are subject to collection and analysis of extensive quantities of personal information for immigration control and ancillary purposes. This information is aggregated and stored for long retention periods in networks of databases and shared among an escalating number of public and private actors with limited transparency, oversight, or accountability.

These technologies have been deployed in the context of a well-documented, long-term expansion of immigration enforcement in the United States. By any measure, enforcement levels have soared in recent decades. Federal expenditures on border and immigration control have grown fifteen-fold since the 1980s and now substantially exceed expenditures on all other federal law enforcement programs combined. These programs have been supplemented by a dizzying array of initiatives, often administered by state, local, and private actors, that indirectly regulate immigration by restricting access to rights, benefits, and services—including employment, social services, driver's licenses, transportation services, education, and even housing—based on citizenship or immigration status. Increasingly, immigration control objectives also are pursued through criminal prosecutions. Importantly, while these programs have been initiated and implemented as immigration control measures, many of these measures necessarily operate upon and are experienced by both noncitizens and U.S. citizens alike Increasingly, many of these initiatives also are being deployed to serve a range of other, non-immigration-related purposes.

The proliferation of these initiatives has contributed to a staggering, widely noted increase in the number of individuals deported from the United States. Less appreciated in the United States, however, has been the revolution taking place in the techniques and technologies of immigration control themselves—their swift proliferation, enormous scale, likely entrenchment, and broader significance.[2] While these tools of the "automated administrative state" (Citron 2008) have facilitated the expulsion of countless numbers of noncitizens, they also more fundamentally have reshaped the meanings and functions of immigration control itself—transforming and integrating a regime of *immigration enforcement*, operating primarily upon noncitizens at the territorial border, into part of a more expansive regime of *migration and mobility surveillance*, operating without geographic bounds upon citizens and noncitizens alike. (Kalhan 2014, 2013)

The New Surveillance Infrastructure of Immigration Control

New technologies have reconfigured four distinct sets of functions that run through all of these immigration control initiatives: *identification*, *screening and authorization*, *mobility tracking and control*, and *information sharing*. These technologies have routinized the collection, storage,

[1] For detailed treatment of the issues discussed in this submission, see Kalhan 2014, 2013, 2008.

[2] Scholars examining immigration control in Europe, by contrast, have been more attuned to these developments. (E.g., Brouwer 2008; Guild 2009)

aggregation, processing, and dissemination of detailed personal information for immigration control and secondary purposes on an unprecedented scale. The ramifications of this reconfiguration may be seen in a variety of concrete domains—including territorial border control by federal officials, interior enforcement by state and local officials, and employment eligibility verification by private employers. In each of these settings, automation, algorithms, and technology-based surveillance not only have contributed to tremendous growth in the number of individuals removed from the United States, but also have significantly transformed how immigration control activities are conducted, experienced, and resisted.

These broad expansions in the scope of immigration enforcement, together with major investments to construct the technological infrastructure to support those expansions, have given rise to what may be described as the *immigration surveillance state*. (Kalhan 2014) In its current incarnation, the immigration surveillance state has most visibly facilitated a regime of mass detention and deportation. However, as an approach to governance, immigration surveillance runs much deeper, encompassing a broader range of activities that both restrict *and* facilitate migration and mobility of both noncitizens and U.S. citizens, both within and outside the United States. Proposals for legalization of unauthorized migrants, for example, are not only unlikely to slow or reverse the development of the immigration surveillance state, but in fact are likely to consolidate and extend its reach, since the logic of surveillance—and of making unauthorized migrants legible and visible to the state—is embedded within most contemporary legalization proposals themselves.

On a relatively limited scale, the Obama administration's Deferred Action for Childhood Arrivals program offers a glimpse at how immigration reform may reinforce the immigration surveillance state. Strictly speaking, DACA involves a categorical but temporary exercise of prosecutorial discretion, but the "DACAmented" status it confers may be understood as a form of quasi-legalization. (Kalhan 2015) The program permits unlawfully present noncitizens under the age of thirty-one to request a renewable, two-year period of temporary relief from deportation and employment authorization if they arrived in the United States while below age sixteen; have continuously resided in the United States since June 15, 2007; are currently enrolled in school, graduated from high school or a GED program, or received an honorable U.S. military discharge; have not been convicted of certain specified criminal offenses; and do not otherwise present any threat to national security or public safety. DACA applicants must submit documentation to the government establishing their identity and fulfillment of these eligibility criteria. In addition, the government collects detailed biographic information and biometrics (photographs, fingerprints, and signatures) from all applicants in order to conduct criminal history and national security background checks against various government databases and to enroll individuals into those systems if their biometric records are not already included.

At least within the current terms of debate in the United States over immigration policy, any legalization program that Congress ultimately might adopt to permit unauthorized migrants to become legal residents would invariably require, albeit on a much larger scale, similar processes of data collection, processing, storage, and dissemination of personal information. While legalization often is framed in public discourse as a means of advancing justice, compassion, and human dignity, advocates and policymakers increasingly characterize legalization as a means of achieving instrumental objectives closely tied to the logic of immigration surveillance—for example, minimizing the social harms that arise from a large underground shadow population and enabling authorities to know who is present within the country. With these pragmatic concerns front and center, the task of making unauthorized noncitizens visible and legible to government authorities invariably becomes a central objective in any legalization scheme. To that end, the logic, practices, and institutions of immigration surveillance—of identification, screening and authorization, mobility tracking and control, and information sharing—also become critical.

The Consequences of Immigration Surveillance

While the regulation of migration necessarily involves some monitoring and surveillance of immigration and citizenship status, the largely unimpeded expansion of immigration surveillance has eroded the legal principles and practical mechanisms that traditionally have constrained the exercise of power in immigration control. In an era of immigration surveillance, limiting the circumstances in which immigration control activities take place—and thereby allowing immigration and citizenship status and other personal information to remain invisible, irrelevant, and protected from use in a broader range of day-to-day settings—serves valuable social interests.

The expansion of technology-based surveillance has contributed to significant changes in how immigration and citizenship status helps to constitute an individual's public identity and social visibility. While status has always mattered deeply when determining an individual's entitlement to certain rights and benefits, in many if not most day-to-day contexts status has traditionally remained legally and socially irrelevant, invisible, and effectively private. However, the technology-driven proliferation of immigration control activities by federal, state, local, and even private actors has rendered status visible, accessible, and salient in many more domains than ever before.

As such, the expansion of immigration enforcement—and the implementation of new surveillance and dataveillance technologies within those enforcement initiatives—implicates underappreciated privacy-related questions for both citizens and noncitizens that are comparable to those arising in many other areas of contemporary governance. Collectively, these initiatives dramatically expand the day-to-day circumstances in which individuals must disclose their status and demonstrate that their presence is legally authorized. In an ever-widening array of settings, these initiatives all require collection and verification of information about immigration and citizenship status and other personal information from citizens and noncitizens alike. To implement these mandates in an integrated manner, officials have developed powerful systems to store, aggregate, and disseminate that information across all of these programs and beyond.

The result has been to accelerate the deterritorialization of the national border for migration and mobility control purposes. As these immigration surveillance activities have proliferated and become tightly integrated with each other, the set of boundary points at which the nation-state authorizes individuals to enter or be admitted, prevents or allows their entry or admission, or subjects them to possible expulsion has been decoupled from the territorial border and rendered "virtual": layered, electronic, mobile, and policed by an escalating number of public and private actors, largely free from the practical and legal mechanisms that have traditionally constrained immigration and border control activities. The expansion of immigration surveillance thereby disrupts the traditional mechanisms that have negotiated the tension between law's exclusionary impulses, in which immigration status is deemed an appropriate basis upon which to make distinctions, and its more inclusive impulses, in which status is regarded as playing no legitimate role.

The technologies that enable immigration surveillance are not inherently harmful—indeed, many of them can and do bring significant benefits. However, as illustrated in debates over technology-based surveillance in other contexts, the unimpeded expansion of these mechanisms erodes both the legal principles and the practical mechanisms that have traditionally constrained aggregations of power and protected individual autonomy and privacy. (Marwick 2014; Gilliom and Monahan 2013; Balkin 2008; Lyon 2007; Marx 2002; Solove 2001) In the immigration context, those constraints have always been less robust in the first place, creating precisely the circumstances in which mistreatment of individuals or groups on the basis of race, religion, national origin, or immigration and citizenship status can take place without opportunities to be challenged or remedied.

Constraining Immigration Surveillance

With the technologies and processes of the immigration surveillance state becoming a more durable part of the landscape of immigration regulation, much greater attention needs to be given to principles and mechanisms to constrain, inform, and guide their implementation, with greater transparency and oversight, to preserve circumstances in which immigration control and surveillance activities do not take place and ensure greater due process, transparency, and accountability when they do.

Immigration surveillance demands reassessment of the interests at stake when personal information and travel history are collected, maintained, analyzed, and disseminated for purposes related to immigration control and the mechanisms to protect those interests. The proliferation of zones where immigration control activities take place—and where detailed information on individuals and their migration and mobility histories is collected and subsequently aggregated, stored, and disseminated—carries a range of social costs. While it may be entirely appropriate to collect, maintain, and disseminate personal information for immigration control purposes in some contexts and subject to certain constraints, both individuals and society as a whole have legitimate interests in preserving zones in which these immigration surveillance activities do not take place and in making sure that when they do take place those activities are appropriately limited and constrained.

To some extent, those interests are individual interests, stemming from the value of preserving individual anonymity or quasi-anonymity more generally and the individual harms that can result when individuals' migration and mobility are routinely tracked and detailed information is maintained. But they also arise from a broader set of social concerns—for example, preventing coercive or excessive aggregations of unrestrained government and private power—which often have less to do with the particular information being collected in any given instance than with the harms that can arise from the means of surveillance and information management.

Vindicating these interests requires context-appropriate constraints on the collection, use, storage, and dissemination of personal information for immigration control purposes—including robust limits on retention periods and secondary uses of information that were not originally contemplated. To date, however, exuberance over the potential benefits of interoperable databases and other new technologies has clouded attention to the continued importance of these limits when implementing these systems for migration and mobility control purposes.

Moreover, in a world in which the migration border is effectively everywhere, policed by large numbers of actors other than national immigration officials—and in which immigration surveillance activities reach large numbers of individuals, including noncitizens and citizens alike—the traditional legal rationales for sweeping deference to government actors in border, migration, and mobility control become more difficult to maintain. The categories of potential deprivations that can result from immigration surveillance activities have multiplied drastically beyond the simple ability to enter and remain in the country. With the expansion of the domains of enforcement and the tools of immigration surveillance, these enforcement activities can place restrictions on the rights to international and domestic travel, employment, education, social service benefits, and freedom from physical restraint in both the criminal justice and immigration enforcement processes. As discussed above, the powerful tools of immigration surveillance create significant risks of erroneous deprivations and are easily susceptible for uses beyond those originally contemplated when implemented.

Finally, immigration surveillance demands greater attention to transparency, oversight, and accountability. Whether programmatically or in the context of individual adjudications, immigration agencies, although improving in some ways, have long suffered from major transparency and accountability deficits. Those deficits are amply evident in immigration surveillance initiatives and have been exacerbated by the blurred lines created by the deterritorialized migration border. Ensuring greater transparency, oversight, and due process requires responses at a number of different levels.

First, a major contributing factor to the lack of sufficient transparency, oversight, and accountability has been the lack of sufficiently concrete or detailed legal authority to support and guide such major and complicated initiatives. No framework statutes govern or constrain many immigration surveillance activities in the United States. This lack of a statutory framework governing surveillance activities that implicate privacy interests in migration, mobility, and travel data stands in marked contrast to other areas, such as communications and financial services, in which government access, storage, and dissemination of personal information have long been governed and constrained by framework statutes. Accountability and oversight of immigration surveillance would be better served by a more detailed, coherent legal framework governing immigration surveillance activities and opportunities for greater public engagement with those rules.

Second, individual opportunities to redress harms arising from immigration surveillance activities, whether administrative or judicial in nature, can still play an important role—not only in remedying individual harms, but also in creating incentives for government actors to ensure that information maintained in their database systems is accurate and complete. Current redress mechanisms, however, do not give sufficient opportunities for individuals to challenge and remedy improper deprivations.

Finally, immigration surveillance demands more attention to forms of structural oversight. Because of the necessarily opaque manner in which database systems and automated decisionmaking mechanisms often function—and the ways in which multiple actors are involved in their operation over extended periods of time—oversight of these systems can be particularly difficult in the context of individual cases. This is undoubtedly more true in the immigration enforcement system, which has traditionally been ill-equipped to supervise investigatory practices. Given the limitations in the ability of individual redress mechanisms to fully ensure proper oversight of database systems, these systems raise the stakes in making sure that structural oversight mechanisms operate effectively. Especially as immigration surveillance integrates the institutions of immigration control with each other and with the institutions of other domains, the blurred lines of accountability among different institutions make accountability difficult; the implementation of automated immigration surveillance initiatives only blurs those lines further.

A complete understanding of immigration governance today must account for how the evolution of enforcement institutions, practices, and meanings has not simply increased the number of noncitizens being detained and deported, but has effected a more fundamental transformation. With the introduction of new surveillance and dataveillance technologies, the traditional relationships between individuals and the institutions of immigration control are being reconfigured in fundamental ways for both noncitizens and citizens alike. And yet, compared to other aspects of the expansion of immigration enforcement, these shifts in migration and mobility surveillance have garnered exceedingly little attention, analysis, or concern—even as vigorous debates about surveillance and dataveillance by public and private institutions have emerged in other settings. As the institutions of immigration surveillance rapidly become integrated into the broader surveillance state, scholars, policymakers, advocates, and community members should grapple more directly with the implications of that reconfiguration.

References

Balkin, Jack M. 2008. "The Constitution in the National Surveillance State." *Minnesota Law Review* 93: 1.

Brouwer, Evelien Renate. 2008. *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*. Brill.

Citron, Danielle Keats. 2008. "Technological Due Process." *Washington University Law Review* 85: 1249.

Gilliom, John, and Torin Monahan. 2013. *SuperVision: An Introduction to the Surveillance Society*. University of Chicago Press.

Guild, Elspeth. 2009. *Security and Migration in the 21st Century*. Polity Press.

Kalhan, Anil. 2008. "The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement." *U.C. Davis Law Review* 41: 1137, *available at* http://klhn.co/41UCDavisLawReview1137.

———. 2013. "Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy." *Ohio State Law Journal* 74: 1105, *available at* http://klhn.co/74OhioStateLawJournal1105.

———. 2014. "Immigration Surveillance." *Maryland Law Review* 74: 1, *available at* http://klhn.co/immigrationsurveillance.

———. 2015. "Deferred Action, Supervised Enforcement Discretion, and the Rule of Law Basis for Executive Action on Immigration." *UCLA Law Review Discourse* 63: 58, *available at* http://klhn.co/deferredaction.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Polity.

Marwick, Alice E. 2014. "How Your Data Are Being Deeply Mined." *N.Y. Rev. Books*, January 9, 2014. http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/.

Marx, Gary T. 2002. "What's New About the 'New Surveillance'? Classifying for Change and Continuity." *Surveillance & Society* 1(1): 9.

Solove, Daniel J. 2001. "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review* 53: 1393.