EXECUTIVE BOARD
EDITOR-IN-CHIEF
Emily Heim

ASSISTANT EDITORS-IN-CHIEF
Rebekah Allison
Kimano Edwards

MANAGING EDITOR
Bobby Desmond

ASSISTANT MANAGING EDITOR
Ashley Genoese

COMMUNICATIONS EDITOR
Michael Shepherd

SENIOR STUDENT WORKS EDITOR
Andrea Gillen

ASST. STUDENT WORKS EDITOR
Ellyse Collins

SENIOR ARTICLES EDITOR
Ralston Mateo

ASSISTANT ARTICLES EDITOR
Joshua Resnick

SENIOR NOTES EDITOR
Sofia Rattes

ASSISTANT NOTES EDITORS
Shannon Anderson
Andrew Bayudan
Richard Russo

GALLEYS EDITORS
Ben Graef
Jacob Post

GENERAL MEMBERS
Stephen Bell
Peggy Brunner
Ashley Chin
Elpidio Cruz
Kimano Edwards
Michael Farhat
Daniel Flood
Michael Friedman
Geneva Hernandez
Ryan Hernandez
Mark Hudson
Matthew Hutchisson
Natasha Jackson

Michael Kassem
Daniel Kersey
Carlos Lievano
Michael Liles
Abraham Oxner
Ryan Peterson
Deron Roberson
John Rutledge
Patrick Salmon
Mariya Solomi
Bradley Spivey
Thai Vo
Joshua Walters

FACULTY ADVISOR
Stacey Steinberg

STAFF EDITOR
Victoria A. Redd
YOUR SPYING SMARTPHONE: INDIVIDUAL PRIVACY IS NARROWLY STRENGTHENED IN CARPENTER V. UNITED STATES, THE U.S. SUPREME COURT’S MOST RECENT FOURTH AMENDMENT RULING

Vania Mia Chaker, Esq.*

Abstract

Recently, the United States Supreme Court wrestled with the profoundly complex and bedeviling issue of individual privacy in the landmark case of Carpenter v. United States.¹ It is the most recent in a long line of Fourth Amendment cases that examine an individual’s reasonable expectation of privacy. In Carpenter, the Supreme Court revisited and expanded upon this query from Riley v. California² and United States v. Jones³—both progeny of Katz v. United States,⁴ the leading case in this area.

The Carpenter Court ruled the government required a warrant before it could use private information arising from defendant Timothy Carpenter’s cellular phone⁵—specifically, his cell site location information (CSLI). In the 5-4 decision, the Court ruled “narrowly” in favor of privacy, finding the government had constitutionally violated Mr. Carpenter’s reasonable expectation of privacy by acquiring this private

---

⁵ Carpenter, 138 S. Ct. at 2221.

* A.B., Stanford University; M.B.A., Columbia Business School; M.B.A., University of California, Berkeley Haas School of Business; J.D., University of California, Berkeley School of Law.

I am deeply grateful to all of the gracious individuals who have assisted me with this project, but especially long-time mentors, Dean Emeritus Jesse Choper, the Honorable Tom Campbell, and the Honorable Christopher Cox. Without their invaluable assistance and interest in my work, this Article would never have reached fruition.

I owe a profound debt of gratitude to all of my beloved mentors, my esteemed advisors in academia and law, and my inspiring Stanford professors, including the Honorable Edwin Meese III, the Honorable Christopher Cox, the Honorable Tom Campbell, the Honorable Lane Evans, the Honorable Rudi M. Brewster, the Honorable Mitchel R. Goldberg, the Honorable Dick Thornburgh, the Honorable Robert W. Naylor, Professor Lawrence M. Friedman, Ralph N. Schmidt, and all of the distinguished Senior Fellows at the Hoover Institution who I was extremely privileged to have worked with and known. A special, heartfelt thank you goes to Jonathan A. Sebastiani, Donald L. Lucas, Sr., and Kimberly R. Hauser. I am extremely fortunate and grateful to have had the encouragement and support of all of these fine individuals during my career.

I also thank Ryan G. Baker, Matthew M. Mahoney, Phil Burkhardt, Jaime Marquart, Charles L. Deem, and William V. Whelan for their steadfast support.

I dedicate this Article to Henri, Jeanne, Alberit, Colette, and Lucien Chaker, M.P.B., B.B.L. – et toutes les personnes qui j’appelle ma famille.
information without a warrant. It ruled that, as a cell phone customer, Mr. Carpenter could reasonably expect that his CSLI would be treated as private, even though it was in the possession of a third party. In so ruling, the Court declined to apply the long-standing third-party doctrine of United States v. Miller and Smith v. Maryland. These cases, which stand for the proposition that there is a reduced expectation of privacy in information an individual knowingly shares with another, have thus been narrowed.

Against a backdrop of stunningly advanced surveillance technology and the strictures of the United States Constitution, the question of how individual privacy comports with the need for police investigation is a complex and impressively difficult one. In the current political landscape, judicial vigilance becomes increasingly important in protecting the appropriate dimensions of individual privacy. The grave risks of governmental abuse may militate in favor of strengthened judicial oversight in determining the parameters of the state’s broad investigative powers. Strong privacy protections may indeed serve to function as a safeguard against the risks of governmental overreach, police misconduct, and improper warrantless surveillance.

INTRODUCTION ................................................................. 3

I. DIGITAL TECHNOLOGY AND THE QUALITATIVELY DIFFERENT NATURE OF PRESENT-DAY CELLULAR DEVICES ....................... 5

II. THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE UNDER KATZ AND THE RECENTLY EVOLVING FOURTH AMENDMENT LANDSCAPE .................................................. 7

III. THE THIRD-PARTY DOCTRINE ........................................... 9

IV. THE HIGHLY INTRUSIVE NATURE OF DIGITAL TECHNOLOGY MAY POTENTIALLY LEAD TO A FURTHER NARROWING OF THE THIRD-PARTY DOCTRINE ...................................................... 12

V. IS THE GOVERNMENT’S VAST ARRAY OF AGGRESSIVE—AND HIGHLY INTRUSIVE—COVERT SURVEILLANCE PRACTICES CONSTITUTIONAL? ................................................................. 14

VI. THE COURT’S CALCULUS OF PRIVACY IN A SOCIETY MARKED BY INCREASING GOVERNMENT SURVEILLANCE ...................... 16

6. Id. at 2219.
7. Id. at 2220.
INTRODUCTION

The United States Supreme Court again wrestled with the profoundly complex and bedeviling issue of individual privacy in the landmark case of Carpenter v. United States. It is the most recent in a long line of Fourth Amendment cases that examine an individual’s reasonable expectation of privacy. In Carpenter, the Supreme Court revisited and expanded upon this query from Riley v. California and United States v. Jones—both progeny of Katz v. United States, the leading case in this area. In the 5-4 decision, Chief Justice John Roberts delivered the opinion of the Carpenter Court in favor of individual freedom, in which Associate Justices Ruth Bader Ginsburg, Stephen Breyer, Sonia Sotomayor, and Elena Kagan joined.

The Carpenter Court ruled the government required a warrant before it could use private information acquired from defendant Timothy Carpenter’s cellular phone—specifically, his cell site location information (CSLI). The Court ruled “narrowly” in favor of privacy, finding the government had constitutionally violated Mr. Carpenter’s reasonable expectation of privacy by acquiring this private information without a warrant. It ruled that, as a cell phone customer, Mr. Carpenter could reasonably expect that his CSLI would be treated as private, even though it was in the possession of a third party. In so ruling, the Court declined to apply the long-standing third-party doctrine of United States v. Miller and Smith v. Maryland. The holdings in these cases, which stand for the proposition that there is a reduced expectation of privacy in information an individual knowingly shares with another, have thus been

---

15. Carpenter, 138 S. Ct. at 2221.
16. Id. at 2219.
17. Id. at 2220.
narrowed. Because of this striking departure from prior precedent, Carpenter is considered a landmark decision.

Justices Anthony Kennedy, Neil Gorsuch, Clarence Thomas, and Samuel Alito, however, roundly criticized the opinion. Justice Thomas filed a dissenting opinion, and Justice Alito filed a dissenting opinion in which Justice Thomas joined. Justice Gorsuch also filed a dissenting opinion. The dissenting Justices seemed most concerned with what they considered the majority’s lack of clear guidance and specificity as to what would constitute constitutional conduct during a police investigation. Some Justices also expressed concern that law enforcement’s legitimate need to investigate its cases could be compromised. Justice Alito, for example, stated that he believed the decision may imperil many valuable and entrenched investigative practices upon which law enforcement has historically relied—a worry echoed by other dissenting Justices. As Justice Kennedy quoted from Riley to explain: “In short, the Court’s new and uncharted course will inhibit law enforcement and ‘keep defendants and judges guessing for years to come.’” He deemed this to be a grave consequence for the “proper administration of justice.”

A common, overshadowing thread in the dissenting opinions seemed to center around the extent to which the scope of the third-party doctrine


22. Justice Kennedy, for example, wrote, “the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line.” Carpenter, 138 S. Ct. at 2234 (Kennedy, J., dissenting). Justice Kennedy went on to note: “The Court’s multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness—puts the law on a new and unstable foundation. Id. Justice Thomas stated: “Suffice it to say, the Founders would be confused by this Court’s transformation of their common-law protection of property into a ‘warrant requirement’ and a vague inquiry into ‘reasonable expectations of privacy.’” Id. at 2244 (Thomas, J., dissenting).

23. Justice Alito warned: “I share the Court’s concern about the effect of new technology on personal privacy, but I fear that today’s decision will do far more harm than good. The Court’s reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.” Id. at 2246–47 (Alito, J., dissenting).

24. Id. at 2234 (Kennedy, J., dissenting) (internal quotation marks omitted) (quoting Riley v. California, 573 U.S. 134 S. Ct. 2473, 2493 (2014)).

25. Justice Kennedy noted: “[T]he Court fails even to mention the serious consequences this will have for the proper administration of justice.” Id. at 2234 (Kennedy, J., dissenting).
would be narrowed as well as how and where to draw these new constitutional boundaries. It is not entirely clear in what way the government’s reliance on the third-party doctrine will be affected in future cases.

Perhaps in an attempt to assuage the dissenting Justices’ concerns, Chief Justice Roberts emphasized the ruling should only be considered a “narrow”—or limited—win for individual privacy. The question of exactly where to judicially delineate the parameters of privacy is one that is far from over, however, particularly given the significant fissure in the Court regarding such issues. This query may become more complicated by the change in the composition of the Bench in the wake of Justice Kennedy’s retirement and the confirmation of the most recently appointed Justice to the Supreme Court. President Trump is likely to nominate a judge that is significantly more politically conservative than Justice Kennedy, who was often a swing vote in close decisions. Justices’ views on privacy are notoriously idiosyncratic, however. Kennedy, a “moderate,” was anti-privacy in the Carpenter case while Roberts, a “conservative,” was pro-privacy.

Moreover, given the tenuous 5-4 majority, it is not a foregone conclusion that the same line of reasoning—or even a similar ruling in favor of privacy—will prevail during the next Fourth Amendment challenge. In already murky and uncertain waters, the change in the composition of the Bench further underscores the fragile nature of the alliance that formed in Carpenter, which only narrowly tempered the government’s warrantless investigative reach.

I. DIGITAL TECHNOLOGY AND THE QUALITATIVELY DIFFERENT NATURE OF PRESENT-DAY CELLULAR DEVICES

Some facts may help contextualize this important ruling. In 2013, Timothy Carpenter was convicted of robbing Radio Shack and T-Mobile stores where—ironically—he stole smart phones. Because a firearm was involved in the commission of the crimes, the district court sentenced him to 1,395 months, or 116.25 years, in federal prison. During its investigation, the government had obtained extensive location information from Mr. Carpenter’s cellular phone, evidence which the

26. Id. at 2220 (“Our decision today is a narrow one.”).
27. As of the writing of this Article, Judge Brett Kavanaugh, a judge for the U.S. Court of Appeals for the D.C. Circuit, has been nominated by President Trump to fill the vacancy left by Justice Kennedy. Judge Kavanaugh is considered by most to be a politically conservative judge. See, e.g., The Path Ahead for Supreme Court Nominee Brett Kavanaugh, WASH. POST, https://www.washingtonpost.com/graphics/2018/politics/supreme-court-justice-nominations/?noredirect=on&utm_term=.2a4f5a16eef (last updated July 9, 2018).
29. Id. at 2213.
government then used to convict him. Specifically, the government obtained 12,898 location points tracking Mr. Carpenter for over 127 days. Interestingly, only four of those location points placed Mr. Carpenter near cell sites where the robberies had occurred.

Technology is certainly our friend, but it is also capable of alarming intrusions and insidious insinuations into our personal lives. The very same technology that has become deeply entrenched into the fabric of daily life can be used to surreptitiously surveil and monitor those who rely on it in ways few could ever have imagined. In its opinion, the Court discussed the constitutionality of the government’s warrantless use of the personal information that could be gleaned from “spying smart phones,” including the CSLI at issue.

The Carpenter Court found the ease with which the government can use smart phones to monitor people’s whereabouts throughout the entirety of each day, and then store that information for lengthy periods of time, to be profoundly troubling. The Court ruled the use of such “deeply revealing” information—that had been obtained without a warrant—to be unconstitutional under two lines of legal doctrine. First, the government’s use of the CSLI data violated a person’s reasonable expectation of privacy under a Katz analysis. Second, it fell awry of the third-party doctrine under the Miller and Smith line of cases.

In rendering its decision, the Court focused greatly on the public’s ubiquitous reliance on cellular phones and the great breadth of information that can be obtained from them. The Court observed that personal devices are in widespread use with the vast majority of people relying on them on a daily, if not continual, basis. It also looked to the fact that cellular phones are qualitatively far different today from analog phones—or even cellular phones of a prior generation. These spying smart phones enable the government to obtain a tremendous amount of

30. Id. at 2212–13.
31. Id. at 2212.
32. Id. at 2213.
33. Id. at 2217–19.
34. See id.
35. Id. at 2223.
36. Id. at 2214–15.
37. Id. at 2217–19.
38. Id. at 2219–220.
39. Id. at 2211 (“There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.”).
40. Id. at 2217–18.
41. Id. at 2218.
42. Id. at 2217.
information about their users, which includes location data as well as a plethora of other personal information.\(^{43}\)

Smart phones also often allow access to computer files and other personal information that is virtually stored in “the cloud.”\(^{44}\) Cellular phones have become mini-computers, cameras, stereo systems, telephones, alarm clocks, fitness trackers, and countless other consumer devices—all rolled into one pocket-sized, but very powerful and seemingly omniscient, device. A smart phone’s functionality, however, necessarily relies upon the owner’s private and often highly sensitive personal information. Bank account balances, credit card account numbers, the names and numbers of loved ones, personal photographs, text messages, health and medical history, fitness tracking, location information, access to digital personal and work files, and all sorts of other personal data are all easily accessible from the cellular phones of most individuals.

II. THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE UNDER KATZ AND THE RECENTLY EVOLVING FOURTH AMENDMENT LANDSCAPE

The Court ultimately ruled that the government’s warrantless access to an individual’s CSLI was unconstitutional.\(^{45}\) So let us turn to the first facet of the judicial opinion which focused on a Katz analysis. In Carpenter, as in Riley and Jones, the Court retreated a bit from the Supreme Court precedent that seemed to allow law enforcement somewhat greater latitude in the post-9/11 era.\(^ {46}\) Instead, it harked back to one of the Fourth Amendment’s most famous legal doctrines that has often historically served to narrow law enforcement’s investigative reach. Evoking Katz, the Court reaffirmed that citizens have a reasonable expectation of privacy over highly personal information such as the CSLI at issue in this case.\(^ {47}\)

Some of the same privacy concerns the Court voiced in Jones and Riley resonated in Carpenter.\(^ {48}\) All three cases seem to center on the government’s intrusive access to private information made possible by

---

43. See id.

44. See, e.g., Christopher Soghoian, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 393–97 (2010).

45. See Carpenter, 138 S. Ct. at 2221.


47. Carpenter, 138 S. Ct. at 2217.

48. Although the Court’s decision in Jones ultimately turned on a property rights analysis as discussed in the Knotts and Karo line of cases, similar threads of concerns regarding an individual’s expectation of privacy arose in Jones, Riley, and Carpenter. See id. at 2217–19; Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Jones, 132 S. Ct. 945, 949–52, 955–57, 963–64 (2012).
technological advances.\textsuperscript{49} Chief Justice Roberts emphasized in \textit{Carpenter}, as he did in \textit{Riley}, that the public’s ever-greater reliance on digital technology is a reality of modern life. Moreover, the widespread use of cell phones, which contain the “privacies of life,”\textsuperscript{50} makes individuals’ sensitive information particularly susceptible to intrusion.

Not only do cell phones allow access to a great amount of personal information and sensitive data, but cellular phones are often figuratively—if not literally—joined at the hip of their owners. This affords the government a wealth of additional information that derives specifically from the location data.\textsuperscript{51} Given that most people carry their phones with them virtually everywhere, Justice Roberts observed that cell-site location records essentially provide the government with “near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”\textsuperscript{52} This data enables the government to learn precisely where the phone—and thus the person—has been and at what time—as well as what other cellular phones were in the same area at that same time.\textsuperscript{53} The \textit{Carpenter} Court made specific reference to the highly intrusive nature of such information, which it characterized as the “detailed, encyclopedic and effortless” tracking of a person using CSLI data.\textsuperscript{54}

The Court’s observation that people would not expect police to track their every movement over long periods of time, which was exactly what cell site location records did,\textsuperscript{55} was pivotal. The Court noted that, as a result of the CSLI, the government was also privy to possibly more sensitive collateral information.\textsuperscript{56} This includes every location a person has traveled and nearly everyone she has met.\textsuperscript{57} Moreover, the Court noted this information was available to law enforcement not only on a going-forward basis but also historically going back five years—\textit{all without a warrant}.\textsuperscript{58}

In \textit{Jones}, the Court expressed similar concern over the government’s ability to warrantlessly track, routinely surveil, and record an individual’s

\textsuperscript{49} See \textit{Jones} at 132 S. Ct. at 953–54, 963–64; \textit{Carpenter}, 138 S. Ct. at 2217–19; \textit{Riley}, 134 S. Ct. at 2493.

\textsuperscript{50} \textit{Riley}, 134 S. Ct. at 2494–95 (2014) (citations omitted) (“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’”).

\textsuperscript{51} \textit{Carpenter}, 138 S. Ct. at 2218.

\textsuperscript{52} \textit{Id.}

\textsuperscript{53} \textit{Id.}

\textsuperscript{54} \textit{Id. at 2216.}

\textsuperscript{55} \textit{Id. at 2217.}

\textsuperscript{56} \textit{Id.}

\textsuperscript{57} \textit{Id.}

\textsuperscript{58} \textit{Id. at 2218}; Amy Davidson Sorkin, \textit{In Carpenter, the Supreme Court Rules, Narrowly, for Privacy}, \textit{New Yorker} (June 22, 2018), https://www.newyorker.com/news/daily-comment/in-carpenter-the-supreme-court-rules-narrowly-for-privacy (“Generally, cell-phone carriers keep such data for five years, but there is no technological limit.”).
every movement that would not have otherwise been subject to public view. Justice Sotomayor worried that warrantless monitoring—such as with a GPS device or a smartphone—could serve to reveal the deeply personal information that derives from location data, such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." This speaks directly to the "privacies of life" and the very core of our being. The same alarm raised in Jones and Riley reemerged in Carpenter. The Court therefore ruled a warrant would first be required for law enforcement to obtain location data from cellular phone carriers since Mr. Carpenter had a legitimate expectation of privacy in such information.

III. THE THIRD-PARTY DOCTRINE

The second dimension of the legal analysis centered around the third-party doctrine, the tenet that a person has no legitimate expectation of privacy in information voluntarily turned over to a third party. The Carpenter Court narrowed its prior holdings in United States v. Miller, which established the third-party doctrine, and in Smith v. Maryland, which extended the third-party doctrine to information related to telephone records.

Justice Lewis Powell’s words in Miller help explain the rationale underlying the third-party doctrine:

The depositor [i.e. an ordinary citizen] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

60. Id. at 955–56; Carpenter, 138 S. Ct. at 2217–18.
61. Jones, 132 S. Ct. at 955 (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).
63. See Carpenter, 138 S. Ct. at 2217–19.
64. Carpenter, 138 S. Ct. at 2221.
65. Id. at 2219–220.
67. Miller, 425 U.S. at 443 (emphasis added) (citations omitted).
In other words, the Miller Court ruled the Fourth Amendment does not preclude the government from obtaining information without a warrant that a person voluntarily provides to a third party.\textsuperscript{68} This reasoning rests on the premise that a person loses his "legitimate expectation of privacy" in information he himself reveals to third parties.\textsuperscript{69} As such, the Miller Court deemed it constitutional that such information be freely passed on to the government.\textsuperscript{70}

The Jones Court declined to overrule the third-party doctrine; however, it voiced stirrings of concern regarding this legal construct that later reemerged more forcefully in Carpenter.\textsuperscript{71} Justice Sotomayor, for example, expressed her unease in her concurring opinion in Jones as follows:\textsuperscript{72}

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

The Court questioned whether individuals would knowingly intend to waive their privacy rights if they allowed third party access to their personal information as they do on a prosaic, everyday basis—often by necessity:\textsuperscript{73}

People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

She concluded in Jones, for example, that "[o]wners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements."\textsuperscript{74}

\begin{thebibliography}{99}
\bibitem{68} Id. at 444–46.
\bibitem{69} See id. at 443.
\bibitem{70} Id. at 443–45.
\bibitem{72} Id. at 956–57.
\bibitem{73} Id. at 957.
\bibitem{74} Id. at 956 (referring to the asterisked discussion of United States v. Karo, 468 U.S. 705, 707 (1984)).
\end{thebibliography}
Justice Sotomayor’s admonition in *Jones* seems to have presaged the *Carpenter* ruling. The *Carpenter* Court voiced skepticism over the third-party doctrine as it did in *Jones*. Given the extensive amount of deeply personal information people typically share with third parties on an everyday basis, the *Carpenter* Court concluded that ordinary citizens would likely not expect such information to be freely available to the government without a warrant. The Court noted how certain third parties maintain encyclopedic knowledge on individuals in a manner that was not possible during the time *Miller* and *Smith* were decided:

Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.

A great degree of the intrusiveness characterizing the government’s investigative practices stems from the highly advanced nature of current technology. Within the context of today’s digital age, advanced technology has allowed the sort of intrusion that had not been previously possible. But this is the reality of our new digital world. The Court remarked that “seismic shifts in digital technology [have] made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period but for years and years.” This is possible because “modern cell phones generate increasingly vast amounts of increasingly precise CSLI.”

The Court concluded that an individual has a legitimate expectation of privacy over such CSLI that he would not intend to renounce only because of a cursory decision to use third party services:

Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection. Whether the Government employs its own

---

75. Id. at 957.
76. Id. at 955–56; *Carpenter*, 138 S. Ct. at 2217–18.
77. *Carpenter*, 138 S. Ct. at 2217.
78. Id. at 2219.
79. See id. at 2218–19.
80. See id.
81. Id. at 2219.
82. Id. at 2212.
83. Id. at 2217.
surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter’s wireless carriers was the product of a search.

The dangers inherent to such trends and the reality of the greatly advanced digital world in which we live may have influenced the Court’s decision. Although the Carpenter Court did not overrule Smith and Miller in their entirety, it also “decline[d] to extend Smith and Miller to cover these novel circumstances.”

Carpenter may foreshadow a further narrowing of the third-party doctrine; and it will be interesting to see whether this contraction continues. The Court may well recognize that the increasing government intrusion possible as a result of ever-advancing technology, coupled with individuals’ unintended relinquishment of private information to third parties, may run afoul of the Fourth Amendment.

IV. THE HIGHLY INTRUSIVE NATURE OF DIGITAL TECHNOLOGY MAY POTENTIALLY LEAD TO A FURTHER NARROWING OF THE THIRD-PARTY DOCTRINE

Notwithstanding the significance of this judicial decision, Chief Justice Roberts specifically characterized it as having a relatively “narrow” reach. He noted, for example, that it does not affect other aspects of the third-party doctrine, such as banking records. It also does not prevent warrantless “real time CSLI information or ‘tower dumps,’” access to cellular tower data in emergencies, or retrieval for “national security reasons.”

Despite this caveat, the Carpenter decision represents an important, albeit narrow, contraction of well-established Fourth Amendment precedent. This decision may therefore set the stage for future legal challenges.

Because the Carpenter Court focused its concern on advanced technologies that allow the government to engage in highly intrusive investigative practices, areas involving warrantless data retrieval seem particularly ripe for future Supreme Court review. Such future challenges could increasingly constrict the scope of the third-party doctrine and further stem the greater investigative latitude the

84. Id.
85. Id. at 2220.
86. See id.; see also United States v. Miller, 425 U.S. 435 (1976).
87. Carpenter, 138 S. Ct. at 2220.
88. Id.
89. Id.; see Sorkin, supra note 58.
90. Carpenter, 138 S. Ct. at 2217–19; see also, e.g., Soghoian, supra note 44, at 386.
government has enjoyed in the post-9/11 era. After all, the public seems to have begun to increasingly tolerate a certain degree of diminution in civil liberties in exchange for a greater sense of safety in a society rife with perceived terrorist threats.

The significant issues expressed in Jones, Riley, and Carpenter make it foreseeable that similar Fourth Amendment challenges are far from over. Cloud computing, for example, seems like another perfect “domain” for improper law enforcement investigation and surveillance that may later result in judicial review.

The shift to cloud computing obviously brings many benefits to law enforcement: significantly reduced manpower requirements, no need to go before a judge or establish probable cause in order to obtain a warrant, as well as the complete elimination of physical risk to agents who might be shot or attacked during a raid.

From the government’s point of view, the potential benefits of such digital investigations are myriad and deliciously tempting. With the advent of cloud computing, a person’s entire digital life can be stored in cyberspace. Since files are already uploaded and stored on third-party servers, the government has far easier and likely greater access to an individual’s digital information than it would with a traditional search of physical items in a home. More importantly, the government can also seek to bypass the warrant requirement and obtain the digital files with a mere subpoena, arguing that the individual had himself turned over the

91. See, e.g., Illinois v. Caballes, 543 U.S. 405 (2005); Kyllo v. United States, 533 U.S. 27 (2001). These cases represent judicial precedent that arguably afforded the government greater investigative latitude. See also, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (affording the government greater investigative latitude in order to fight the “War on Terror”).


93. Soghoian, supra note 44, at 387.

94. Here is one explanation of why this is: “So in this digital age, police often do not need to show probable cause of a crime when they want to find out details about your life that they used to find in your home. Instead, they can get your private files from corporations that store your records on their computers. And instead of a search warrant, the police might just need a subpoena—which is ‘trivially easy to issue,’ says Bankston of the Center for Democracy and Technology. Law enforcement doesn’t need a judge’s approval to obtain subpoenas—prosecutors can sign them on their own, as can authorized employees at federal and state agencies. And law enforcement agents don’t need evidence that there’s likely a crime. They need only to be able to show that the records they want are relevant to an investigation.” Daniel Zwerdling, All Things Considered: Your Digital Trail: Does The Fourth Amendment Protect Us?, NPR (Oct. 2, 2013, 1:00 PM), https://www.npr.org/sections/alttechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment -protect-us.
information to a third party. A government agent would certainly welcome the ability to virtually access a target’s most personal information in cyberspace, conveniently from the comfort of a well-lit, air-conditioned office—perhaps while sipping a cup of coffee. No more cramped late-night stake outs or last minute surveillance runs.

A cloud user—or government interloper—can also effortlessly manipulate, retrieve, and organize a typically extensive array of digital files at its leisure. This includes potentially unlimited, “on demand” access to a complete library of a person’s most private information—including writings, photographs, and financial data—figuratively and literally. Depending on the third-party entity holding the sought-after information, the government could likely access this information with the mere request of a subpoena—a simple stroke of a pen—without the safeguard of a warrant. After all, a subpoena requires very little. A police officer or federal agent need only justify the request according to his department’s own internal policies, which may be faulty or woefully deficient. There is no judicial oversight of the request, and law enforcement is not immune from mistake, impropriety, or abject wrongdoing. The implications of the government’s far-reaching and relatively unfettered access to an individual’s private information are grave and should therefore raise concerns for all.

V. IS THE GOVERNMENT’S VAST ARRAY OF AGGRESSIVE—AND HIGHLY INTRUSIVE—COVERT SURVEILLANCE PRACTICES CONSTITUTIONAL?

The Carpenter Court underscored the concern that investigational practices currently employed by the government are alarmingly—and unlawfully—intrusive. Within this context, the Internet of Things (IoT) is another area of technology ripe for governmental abuse. The IoT affords the public a vast array of conveniences while also concomitantly creating a potential conduit for the government to violate the sanctity of our homes and insinuate itself into our private lives.

“Smart” televisions and other “smart” devices, for example, can monitor and store sounds and conversations that occur inside of the homes in which they are located—including bedrooms, living rooms, and

95. Id.
96. See id.; Soghoian, supra note 44, at 386.
97. See Carpenter, 138 S. Ct. at 2217.
98. Id.
99. Zwerdling, supra note 94.
100. Id.
101. See id.
102. See Carpenter, 138 S. Ct. at 2223.
nurseries.\textsuperscript{104} The audio captured could be highly personal, including, for example, a child’s giggle, a baby’s gurgle, or a lover’s whisper. Samsung has confirmed that “\textit{even if the owner opts out of the voice-recognition feature . . . the set will still capture what is said}.”\textsuperscript{105} But the intrusion does not end there: After capturing those sounds, \textit{these smart devices can possibly transmit that audio to third parties}.\textsuperscript{106} Please allow me to rephrase: Some stranger somewhere might very well have the ability to spy on you or your family’s most private moments as well as gain information about your children and your family’s patterns of life.\textsuperscript{107}

Depending on future judicial interpretations of \textit{Carpenter}, the IoT could possibly bestow the government with a virtual superhighway into the most private areas of our lives. Questions of legality and constitutionality aside, many of us would consider these sorts of covert intrusions quite alarming. To most people, the implications of this are enormous. Many would feel these sorts of intrusions are not just wrong, but truly violating.

Of course, this is but one example. There are myriad other examples of covert surveillance which may potentially be available to police without a warrant. Some retail stores use cameras with facial recognition and surreptitious biometric iris scanning technology that can be easily hidden, for example, in mannequins.\textsuperscript{108} The government itself utilizes long-distance iris scanners to surveil public places and amass biometric information on its citizenry—surreptitiously and without consent.\textsuperscript{109} License plate scanners of automobiles on the roadway and in parking lots are in widespread use, monitoring our movements, driving habits, and travel patterns.\textsuperscript{110} “Eyes in the Sky” have become increasingly common as law enforcement has begun to employ warrantless drone surveillance.


\textsuperscript{105} See id.

\textsuperscript{106} See id.

\textsuperscript{107} See id.; Zwerdling, supra note 94.


\textsuperscript{109} See sources cited supra note 108.

\textsuperscript{110} See \textit{Automated License Plate Readers (ALPRs)}, EFF, https://www.eff.org/pages/automated-license-plate-readers-alpr (last visited Aug. 31, 2018) (“Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server.”).
programs.\textsuperscript{111} The government has monitored electronic communications and accessed the stored data of individuals, including emails and computer files—all surreptitiously and without consent.\textsuperscript{112} Indeed, the government has quietly built a series of warehouses of truly immense proportion in the Utah desert\textsuperscript{113} to store the vast amounts of metadata it has compiled on its citizens.\textsuperscript{114}

VI. THE COURT'S CALCULUS OF PRIVACY IN A SOCIETY MARKED BY INCREASING GOVERNMENT SURVEILLANCE

Against a backdrop of stunningly advanced surveillance technology and the strictures of the United States Constitution, the question of how individual privacy comports with the need for police investigation is a complex and impressively difficult one. In the current political landscape, judicial vigilance becomes increasingly important in protecting the appropriate dimensions of individual privacy. The grave risks of governmental abuse may militate in favor of strengthened judicial oversight in determining the parameters of the state’s broad investigative powers. Strong privacy protections may indeed serve to function as a


\textsuperscript{112} See, e.g., James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html; James Risen & Eric Lichtblau, Spying Program Snared U.S. Calls, N.Y. TIMES (Dec. 21, 2005), https://www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html (“A surveillance program approved by President Bush to conduct eavesdropping without warrants has captured what are purely domestic communications in some cases, despite a requirement by the White House that one end of the intercepted conversations take place on foreign soil, officials say.”) (emphasis added). See generally NSA Spying: How It Works, EFF, https://www.eff.org/nsa-spying/how-it-works (last visited Aug. 31, 2018) (“In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades.”).

\textsuperscript{113} The government’s Stellar Wind Program is located at Camp Williams near Bluffdale, Utah. It is also known as the Intelligence Community Comprehensive National Cybersecurity Initiative Data Center. See, e.g., Steve Fidel, Utah’s $1.5 Billion Cyber-Security Center Under Way, DESERET NEWS (June 6, 2011, 1:10 AM), http://www.deseretnews.com/article/705363940/Utahs-15-billion-cyber-security-center-under-way.html.

\textsuperscript{114} Tim Cushing, NSA’s Stellar Wind Program Was Almost Completely Useless, Hidden from FISA Court by NSA and FBI, TECHDIRT (Apr. 27, 2015, 12:34 PM), https://www.techdirt.com/articles/20150427/11042430811/nsas-stellar-wind-program-was-almost-completely-useless-hidden-fisa-court-nsa-fbi.shtml (“A huge report (747 pages) on the NSA’s Stellar Wind program has been turned over to Charlie Savage of the New York Times after a successful FOIA lawsuit. Stellar Wind has its basis in an order issued by George W. Bush shortly after the 9/11 attacks. Not an executive order, per se, but Bush basically telling the NSA that it was OK to start collecting email and phone metadata, as well as warrantlessly tap international calls into and out of the United States.”).
safeguard against the risks of governmental overreach, police misconduct, and improper warrantless surveillance.

It is possible the increasingly intrusive trend of governmental investigative activities in the post-9/11 period helped shape the Carpenter ruling and the resulting slight contraction of the third-party doctrine toward a more appropriate Fourth Amendment equipoise. Although characterized as a “narrow” ruling by the Carpenter Court, its significance could likely be far greater than stated at first blush—especially given the sort of advanced surveillance technology that has yet to come to light. Indeed, the Court may rely on its rationale in the Carpenter decision in the event of future legal challenges of warrantless digital searches where the government invokes the third-party doctrine as justification for those searches. Only time will truly tell. The Court’s decisions in Carpenter, Riley, and Jones, however, could signal the beginnings of a contraction in the progressively greater investigative latitude the government has been enjoying in the post-9/11 era.
I. INTRODUCTION

When creatives talk about their work, they rarely talk about copyright or trademarks. Routines of production, sources of inspiration, and collaborations with colleagues and coworkers figure prominently among their narratives of their own work—but not the legal framing. Yet, the copyright regulation discourse routinely assumes that legal measures are constitutive for creative production. If there is no legal protection for

---

* Senior Researcher, Head of the Research Group Internet Policy and Governance, Alexander von Humboldt Institute for Internet and Society, Berlin, Germany.

creative works, it is assumed creatives will not be able to reap the benefits. In this situation, creatives would lack incentives to create new works in the first place, with the result that they would not innovate at all.

This great discrepancy between the dominant copyright discourse and creators’ own accounts presents a challenge for copyright research. The normative and highly politicized policy debate of the last two decades has paid rather little attention to the concrete practices of cultural production and their commercial exploitation. However, in recent years, empirical research from multiple perspectives has increasingly investigated copyright’s actual effects in the domains of culture and economy: which creative practices it enables or precludes, and how informal norms and discourses complement legal regulation.

In addition to prevailing quantitative approaches and emerging experimental settings, this empirical turn in copyright research has also been driven by qualitative studies that shed light on the practices, routines, and norms of creatives and how these relate to legal provisions such as copyright and patents. The literature on low IP regimes especially provides instructive insights into the different modalities of organizing and regulating the production and circulation of creative goods. In many case studies, scholars have learned that the absence of formal IP protection does not mean the absence of IP control: communities such as French chefs, comedians, and magicians have developed their own set of rules delineating legitimate and illegitimate practices.

In sum, there is ample empirical evidence supporting the position that when seeking to understand the circulation of creative goods there is always more than law involved: these are informal norms, discourses, economic rationales, and the technologies underlying creative practices. These frames may align with copyright provisions, but in many cases they

---


do not. What is still lacking, though, is a theoretical approach to understand and investigate these phenomena within a systematic and comparative framework.

This Essay contributes to empirical copyright research by presenting an integrated governance perspective. This conceptual framework seeks to enable the identification and comparison of different modes of ordering and control in creative production and distribution. Based on sociological institutionalism, this governance perspective does not privilege law ex-ante, but positions norms, discourses, and technology as (analytically) equally relevant dimensions of copyright governance.

The reasoning of this Essay is presented in three parts. Firstly, I draw from Murray to argue against a low IP exceptionalism. The norms and routines ordering creative production in sectors of low IP protection are not unique to these sectors. Instead, they are constitutive of all processes of creative production. Norms and routines are not mere replacements for legal measures in a “negative space of IP.” Instead, it is argued that they are always already present in every form of cultural production and circulation. Thus, the ordering of creative production and circulation is a multimodal process that is realized in many dimensions. Secondly, this perspective is developed into a conceptual framework based on sociological institutionalism (SI) with four modalities of copyright governance: (1) a regulative dimension, addressing the provision and enforcement of formal rules, such as laws, court decisions, terms of services; (2) a normative dimension, investigating the prevalent assumptions about legitimate and illegitimate behavior in a specific community or sector; (3) a discursive dimension, addressing the framings and debates on creativity, authorship, and originality; and (4) a technological dimension that investigates the embodiment of affordances and rules in infrastructures, devices, and algorithms relevant to creative work. This will allow the empirical study of the impact and mutual relations of the different modalities across creative sectors. Finally, to illustrate this concept, the paper discusses the implications of this model for existing case studies on low IP regimes and other sectors.

---

5. See Silbey, supra note 1, at 81–148.
6. Murray et al., supra note 1, at 1.
II. BEYOND LOW IP REGIMES: THERE’S ALWAYS MORE THAN LAW

A. Low IP Regimes: IP Without Law?

This investigation into heterogeneous modes of ordering creative production and circulation takes as its starting point the literature on low IP regimes. In empirical studies, scholars are exploring creative practices and products that are hardly amenable to formal IP regulation. Studies on magicians,8 French chefs,9 comedians,10 and roller derby players11 have demonstrated that there is more than law in controlling and circulating creative work. In the absence of clear-cut legal protection, these communities have developed norms and routines that delineate acceptable from objectionable practices, thus bringing about “Intellectual Property without law.”12 The focus on informal regulation in research addressing these seemingly disconnected fields stems from their legal peculiarity: comedy, magic, and cooking are hardly regulated by formal legal measures. Given this context, stakeholders need to mobilize different modes of regulation other than law in order to coordinate their creative practices and products. In these studies, it is community norms that regulate creative practices and sanction deviant behavior by measures such as exclusion.

By looking at the fashion industry, Raustiala and Sprigman have given this perspective a slightly different spin:13 while this sector is highly monetized and subject to a considerate number of formal regulations (e.g., trademark, design patents), they are able to show that the sector lacks consistent legal rules for its key creative work, fashion design. Intellectual property rights are not able to effectively delineate between legitimate inspiration on the one hand and illegitimate plagiarism on the other hand.14 However, against all assumptions of conventional IP theory, “piracy” does not lead to market failure here but to a flourishing, innovative industry.15

8. Loshin, supra note 4, at 123.
10. Oliar & Sprigman, supra note 4, at 1771–73.
12. Loshin, supra note 4, at 123.
15. Id.
Scholars have addressed a similar puzzle regarding the trade in TV formats. The legal protection of formats is arguably very weak, yet there is a highly profitable global licensing market for formats. Why do organizations pay to license a format that is not consistently protected? Why develop new formats if you can free ride on existing ones? Standard IP theory “would predict that innovators would have no incentive to innovate in such a market. [. . .] [T]he TV format industry would suffer from a significant undersupply of TV formats, as constant free riding on TV format innovation would eliminate incentives to innovate.”

But producers do invest in new formats. There is not much research on this topic, but empirical studies and economic theory suggest that a mix of business strategies, professional practices and community norms drive the necessary level of innovation in this sector. Similarly to the fashion industry, imitation as a form of “herding behavior” generates innovation rather than hindering it. In a multi-method study on imitation and innovation in game production, we identified similar strategies and professional norms. Kate Darling has investigated the strategies of the online adult entertainment industry to cope with a low level of copyright enforcement. Based on qualitative interviews, she has learned that producers shift towards the production of experience goods rather than replicable works. Consumer privacy preferences, consumption habits, low production costs, and a continuing high demand also help this business to thrive sustainably.

In sum, the literature on low IP regimes supports the position that strong community norms can make up for the lack of formal IP regulation. This perspective has been extended to more commercial, and arguably less community-driven sectors, such as fashion, TV formats, game production, and online adult entertainment. While not constituting clear-cut low IP regimes, creative production in these sectors is not easily protected by formal IP regulation, either because it lacks suitable

18. Id.; see also Kretschmer & Singh, supra note 15.
22. Id. at 765–69.
23. Id. at 738–58.
measures to protect the key creative output (fashion, TV formats, games) or effective enforcement (online adult entertainment). Professionals and companies in these sectors complement this, not by strong community norms, but rather by a mix of business strategies, professional norms, and work routines.

B. Against the Exceptionalism of Low IP Regimes: There's Always More than Law

This strand of research routinely presents low IP regimes as the exceptional case; that is, the “negative space of IP” that represents a puzzle in light of standard theory. Similarly, the strategies in the more complex examples of fashion, TV formats, games, and online adult entertainment are regarded as countermeasures to compensate for a lack of copyright protection and enforcement. Taken together, the literature tends to consider these sectors as instructive, yet exceptional cases. In contrast, most creative sectors are well covered by copyright and other IP regulation, so they do not need informal norms or other complementary strategies one might argue.

But this position overlooks some constitutive aspects of ordering creative production and circulation—that there is always more than law. Low IP regimes are only exceptional cases with regard to their legal situation. Beyond a “legal centralism,” a broad set of empirical studies and different humanities theories show us that informal norms, discourses, economic rationales, and technologies of production and circulation always contribute to framing and ordering creative practices whether law provides adequate control or not. As Laura Murray and her co-authors rightly assert, “all creative practices – not merely extraordinary niches like magic and stand-up comedy – features some sort of embodied ideas about attribution, custodianship, and fair practice.”

Studies on game design and a wide range of other creative practices indicate that creators always hold strong concepts of their creative practice and their creative works, sometimes aligning with IP provisions and sometimes not. In fact, many professionals do not know the applicable copyright regulations, and many rarely encounter or explicitly

---

25. Fagundes, supra note 11, at 1098.
26. MURRAY ET AL., supra note 1, at 10.
27. For game design, see Tom Phillips, “Don’t Clone My Indie Game, Bro”: Informal Cultures of Videogame Regulation in the Independent Sector, 24 CULTURAL TRENDS 143 (2015). For other creative practices, see MURRAY ET AL., supra note 1. For the mismatch between IP provisions and Creatives’ perspectives, see SILBEY, supra note 1, at 81–148.
reflect on legal issues in their working routines. David Fagundes’ study on names and branding in roller derby found that informal norms emerge regardless of existing formal IP measures. In her extensive study on creative practices in sectors with mostly strong IP coverage, Jessica Silbey finds strong opinions and informal norms among the interviewees regarding the creative process and the circulation of the creative output. For different aspects and sectors, Silbey identifies mismatches between the creatives’ own positions and formal IP regulation. Especially regarding the creative process, the interviews indicate that copyright and patent law is of very little practical importance. Additionally, experimental studies indicate that creative practices are motivated by a wide array of factors, law being one among many.

So, there is ample empirical evidence for the position that there is always already more than law in ordering creative practices and circulation of creative works. Informal norms and routines do not only complement law in the absence of formal regulation, but they are always involved. Yet, how do these different mechanisms and dimensions interact? How do they mutually reinforce or undermine each other? How can they be included in a systematic and comparative framework for investigating the ordering of creative practices and the circulation of creative works without privileging law ex-ante? This Essay sets out to contribute to the theoretical advancement of empirical copyright research. In the following, I suggest building blocks for a holistic understanding of the governance of creative practices and the circulation of creative works.

III. A GOVERNANCE PERSPECTIVE FOR EMPIRICAL COPYRIGHT RESEARCH

The development of a comprehensive framework for analyzing the ordering of creative practices and the circulation of creative outputs can take different approaches with different theoretical underpinnings. One prevalent and instructive approach is transaction cost economics and its variations in economic and institutional theory. Another one addresses motives and incentives on the individual level of creatives and users of creative products. Psychologically informed research has provided

28. See van Roessel & Katzenbach, supra note 20.
29. Fagundes, supra note 11.
30. Silbey, supra note 1, at 25–54.
insight into the reasoning of individuals creating, using and sharing potentially copyrighted works.

This Essay, in turn, is grounded in sociological institutionalism. The focus in this perspective is neither on individual motives nor on the calculation of transaction costs, but on the processes of developing and contesting shared norms. Put simply, sociological institutionalism is interested in the ways communities or societies negotiate and establish shared expectations about legitimate and illegitimate practices. For copyright research, and specifically for empirical copyright research this promises to provide a useful theoretical avenue. Building on these concepts will allow scholars to integrate the different mechanisms of ordering at play in creative sectors in a systematic and comparative framework. In contrast to psychological and transaction cost frameworks, this perspective focuses on the meso- and macro-levels of negotiating and contesting norms and understanding. It is thus well positioned to integrate formal regulation on the same level.

Institutions, in this line of theory, are not understood as or restricted to formal organizations or rules. Instead they are, in a broader sense, “building-blocks of social order.” They manifest themselves in different forms such as informal norms, daily routines, organizational procedures, common sayings, but also formal regulations. In essence, institutions “represent socially sanctioned, that is, collectively enforced expectations with respect to the behavior of specific categories of actors or the performance of certain activities. Typically, they involve mutually related rights and obligations for actors, distinguishing between appropriate and inappropriate, ‘right’ and ‘wrong,’ ‘possible’ and ‘impossible’ actions and thereby organizing behavior into predictable and reliable patterns.”

This understanding of institutions focuses on the mutual expectations of social actors and suggests different ways and processes that inform these expectations. The classification of practices as right or wrong, appropriate or inappropriate already anticipates the potential of this sort of institutional theory for the endeavor at hand here. Considering norms, discourses and technology as potentially functional equivalents to copyright regulation, this perspective is agnostic to the different possible modalities of substantiating an institution (i.e., of delineating right or wrong, appropriate or inappropriate law is but one factor).

An important element in this line of institutional theory is its sensitivity to less obvious factors of institutionalization. Prominently, sociologists have stressed the cognitive and discursive dimension of

33. Id.
institutions. These dimensions influence behavior not only by normative guidance and by specifying what one should do, but more fundamentally, and maybe even more effectively, by specifying what we imagine that we could do in a given context.\(^\text{34}\) In this perspective, institutions do not primarily consist of “norms and values but [of] taken-for-granted scripts, rules, and classifications.”\(^\text{35}\)

In a recent paper, Dan Burk has analyzed the development and application of patent law from a similar perspective.\(^\text{36}\) Based on sociological institutionalism, he insightfully uncovers the myths and mythology of patent law. His analysis is based on the cognitive dimensions of institutions and thus highlights the prevalent social understandings that bind communities together. Burk argues convincingly that, as narratives that are “true but not factual,”\(^\text{37}\) myths contribute to explaining the “puzzle” of the patent law system that has often been proved ineffective but remains remarkably stable.\(^\text{38}\)

Starting from the same basis, this Essay takes a different route in explaining and investigating matters of intellectual property in context. Burk exclusively focuses on the cognitive dimension of institutions. In contrast, this Essay follows his call to integrate the other “pillars of institutions.”\(^\text{39}\) If successful, this should facilitate a comparative approach focused on the intersection of and interplay between the different dimensions. In turn, the object of explanation here is more restricted than in Burk’s paper. Whereas he delivers a meta-analysis of the consolidation of the patent law system, the framework developed here aims to investigate the classification of actual practices as either legitimate or illegitimate with regard to creative works. In other words, this Essay addresses the governance of creative practices and products. Yet, both are interested in understanding the role of law in social practices,\(^\text{40}\) thus contributing to an instructive shift in perspective. As Silbey pointed out, instead of imposing ex-ante “the view that intellectual property ‘incentivizes’ innovation and creativity, and then showing how IP is not working as it should, a social science investigation asks the empirical question that Burk urges we begin to ask with more determination: ‘[J]ust what roles [are] patents . . . playing?’”\(^\text{41}\)


\(^{36}\) Burk, *supra* note 2.

\(^{37}\) Id. at 429.

\(^{38}\) Id. at 423.

\(^{39}\) Id. at 451.


\(^{41}\) Id. at 347.
The model for the empirical study of social practices and the role of copyright presented here rests on Richard Scott’s typology of institutions, which contains regulative, normative and cultural-cognitive pillars.\(^{42}\) In his synthesis of institutional theories, he summarizes that institutions are “set in motion by regulative, normative, and cultural-cognitive elements.”\(^{43}\) From this perspective of shared expectations, mutually related rights and obligations, and common assumptions about right and wrong, possible and impossible practices are not only constituted by law but also by normative orientations and cognitive framings. As these elements interact, complement, and sometimes conflict with each other rather than constitute separate entities, I prefer to call them dimensions instead of pillars. The enduring and coercive impact of institutions then strongly relies on the coherence of these dimensions, as Marie-Laure Djelic and Sigrid Quack explain: “the stability, robustness and self-reproducing characters of institutions will be all the more pronounced that regulative pressures and systems of control combine with normative and cognitive frames and reinforce each other.”\(^{44}\) Conflicts typically arise when informal norms and formal law or any other dimension diverge with regard to evaluating right or wrong, and appropriate or inappropriate practices.

Turning to copyright, this concept of institutions allows us to develop a multimodal framework to analyze the governance of creative practices and products. This framework posits that there is (1) a regulative dimension, addressing the provision and enforcement of formal rules, such as laws, court decisions, contracts, and corporate policies. In short, copyright as usual. But this is only one of many dimensions and not necessarily a privileged one. There is (2) the normative dimension, describing the prevalent assumptions about legitimate and illegitimate behavior in a specific community or sector (i.e., the community norms in the low IP literature). In addition, institutional theory suggests (3) a cognitive and discursive dimension, addressing the shared (or contested) understandings and framings of issues in certain contexts. An example of the context of copyright relates to the understandings and debates on what constitutes creativity in the first place, the role of originality, or the identification of authorship. While not explicitly present in Scott’s model of institutions, it seems reasonable to add (4) a material or technological dimension that takes into account the affordances and rules embodied in

\(^{42}\) Richard W. Scott, Institutions and Organizations: Ideas and Interests 51 (3d ed. 2008).

\(^{43}\) Id. at 49.

infrastructures, devices, and algorithms relevant to creative work. Scott already concedes that artifacts are important “carriers” for sustaining institutions, but research in Science and Technology Studies (STS) has shown that technologies and artifacts are more active elements in building and constituting social order. They do more than just “embody and represent particular constellations of ideas.” Road bumps, bridges, automatic door closers, or heavy tags on hotel keys are the classic examples in this “sociology of things” that illustrate how artifacts have a strong impact on the way we move, talk, and interact. In this sense, technology is an institutionalized form of social interactions or structures that, once institutionalized, have an effect on the social.

**Figure 1: Layers of Institutions**

This model diverges from prevalent thinking about copyright regulation in two ways. First, it integrates different modes of ordering into a coherent framework for empirical research. Thus, it reflects the findings and arguments stemming from the low IP literature that informal norms and shared beliefs are always involved in creative practices—not only in niche sectors. The relation between these dimensions is not set ex-ante by stating a putative absence of formal regulation and having norms act as a surrogate. Instead, they operate on equal footing. The relation between laws, norms, and discourses then is an empirical
question that is amenable to research. Does copyright law prohibit creative practices that are deemed legitimate within a specific context or across an entire society? Are the understandings and routines of creative production in all creative sectors compatible with the categories of copyright (e.g., authorship, work)? Which creative practices do current or past technologies enable and promote and which ones are constrained, or no longer possible? Does this realm of possibilities align well with informal norms and copyright provisions? In this sense, the legitimacy and robustness of institutions is dependent on the coherence of these dimensions. In sum, this model provides an integrative framework for empirical copyright research that allows us to investigate and compare formal regulations, norms, discourses, and material-technological elements as distinct, yet interdependent modes of copyright governance.

The second feature of this model is that it rests on the notion of governance rather than regulation. While governance as a concept is "notoriously slippery," it provides analytical value in broadening the concept of regulation. At its core, governance refers to all patterns of rule, and exploring governance means exploring the construction of social order and social coordination. Patterns of rule and ordering mechanisms can take different forms and different trajectories, and thus the notion of governance resonates well with the institutional framework presented here. In contrast, the notion of regulation is characterized by intentional and goal-directed interventions into a policy domain. Julia Black defines regulation as "a process involving the sustained and focused attempt to alter the behavior of others according to identified purposes with the intention of producing a broadly identified outcome or outcomes." Regulation may take the form of legislation, private self-regulation or multi-actor arrangements; in all cases, however, it links ordering processes with explicit objectives and measures. Regulatory actors, private or public, assess their options to intervene in a specific field and use the means they deem effective to achieve a desired outcome. Copyright is routinely discussed from a regulatory perspective. What effects do specific provisions have on creative practices or consumption behavior? How can copyright be changed in order to reach desired outcomes? In contrast, the governance perspective

50. With that, it resonates with Burk’s call for agnostically trying to understand what IP really does in practice, not assuming an incentive function (or any other) ex-ante. Burk, supra note 2, at 452; Silbey, supra note 40, at 347.
52. MARK BEVIR, KEY CONCEPTS IN GOVERNANCE 3 (2009).
54. Jeanette Hofmann et al., Between Coordination and Regulation: Finding the Governance in Internet Governance, NEW MEDIA & SOC. 1, 13 (2016).
put forward here focuses on how certain frames and norms constitute, inform, and question the practices of creative people, as well as users of creative products. This complements the prevalent regulatory perspective in important ways, not only because controlling IP involves more than law but also because the reference points of our actions are not solely there to guide our creative practices. Shared beliefs, motives, and legitimizations are not here to regulate our practices; they have emerged in long-term processes and only sometimes they, implicitly or explicitly, inform and guide what we do. In sum, this copyright governance model attributes the ordering and regulation of creative practices to the mutual reinforcement (or weakening) between regulative, normative, discursive, and material elements. Some of which are designed to regulate, but many of which are not.

IV. Modes of Copyright Governance: Regulation, Norms, Discourse, Technology

This Part illustrates the analytical and empirical value of the proposed model by spelling out the kind of questions and answers it enables, and by providing a short application of the model to the governance of imitation and innovation in game development. This illustrative case study is based on a multi-method case investigation: a document analysis of industry handbooks, a discourse analysis of contested cases, and extensive interviews with different professionals and stakeholders from the games sector in Germany. We conducted semi-structured interviews with twenty German game practitioners and four legal consultants and in-house lawyers, taking about ninety minutes each.
TABLE 1: MODES AND LEAD QUESTIONS OF COPYRIGHT GOVERNANCE

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Research Questions</th>
<th>Empirical Account</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulative</strong></td>
<td>Which actors establish which rules (scope!)? How is compliance monitored and deviation sanctioned? How are Rules interpreted and adapted?</td>
<td>Legal Analysis, Policy Documents, Legislation Process</td>
<td>Copyright for Games, Non-Disclosure Agreements, Internal Corporate Policies, Terms of Service of Development Environments</td>
</tr>
<tr>
<td><strong>Normative</strong></td>
<td>With which normative expectations are actors confronted? Which expectations are internalized? How are these norms established and negotiated?</td>
<td>Interviews, Ethnographies, Participatory Observations</td>
<td>Norms within Communities, Comedy, French Chefs</td>
</tr>
<tr>
<td><strong>Discursive</strong></td>
<td>What is “taken for granted”? Construction and deconstruction of shared frames and perspectives</td>
<td>Discourse Analyses, Politicization, Issue Formation, Frames</td>
<td>Debates around “Piracy” and “Stealing” IP, Understanding s of Authorship and Creativity</td>
</tr>
<tr>
<td><strong>Technological</strong></td>
<td>Which rules and assumptions are inscribed into technology? How do services and algorithms structure and regulate our creative practices and our media usage?</td>
<td>Analyses of Technologies, Ethnographies of Tinkering, Digital Methods, User Interactions</td>
<td>Digital Rights Management, YouTube’s Upload-Filtering (Content ID), Development Environment</td>
</tr>
</tbody>
</table>
A. Regulative Dimension

The regulative dimension is the one that is most familiar to scholars of copyright. In addressing the manifest rules and regulations, it is mainly concerned with laws, contracts, court decisions and other legal documents. As an institutional element, the regulative dimension operates essentially in three steps: rule-setting, monitoring, and enforcement. In this view, institutions are accomplished through “the capacity to establish rules, inspect others’ conformity to them and, as necessary, manipulate sanctions—rewards or punishments—in an attempt to influence future behavior.”55 Researching this aspect of governance might be considered business-as-usual for copyright scholarship, hence this Essay will not go into much detail here. Investigating this dimension can include both the substance of rules (e.g., legal analysis) as well as its emergence and implementation (e.g., policy analysis).

In the case study, we were interested in understanding how different modes of governance frame and regulate imitation and innovation in game production. The production of games is characterized by the fact that imitation is a common and necessary industry practice that even spurs innovation. Entire game genres (one can think of platform side scroller games or first-person shooters) have emerged by remaking and extending on great games.56 While the view that imitation is a constituent part of innovation seems to be shared throughout the industry. Recent tussles over alleged clones have sparked lively discussions about legitimate and illegitimate imitation practices in game development.

Interestingly, the legal and regulative dimension is far from providing a clear-cut answer for “navigating this grey zone.”57 Games are composed of several elements (rules, graphics, source code, audio), some of which can be separately protected by intellectual property law. For instance, the source code and audiovisual elements are protected by copyright, while game hardware manufacturers often have their technology patented.58 However, a unique part of games compared to other audiovisual media is the rule-based system. For example, in the case of chess, it is not the exact colors and shapes of the pieces that define the

55. SCOTT, supra note 42, at 52.
57. van Roessel & Katzenbach, supra note 20.
game, it is the possible moves and affordances of the pieces, the actions that emerge from these affordances and the interplay between the actions. Such rule-based systems could arguably be understood as abstract ideas rather than concrete or fixed expressions. As such, games have an “uncopyrightable core: the actual play of the game.” Thus, the long-lasting tension between imitation and inspiration in the games sector and the conflicts around the alleged copying of games is not easily resolved in the regulative dimension.

In the interviews we conducted, we were confronted with a striking neglect of the regulative dimension both with regard to the tension between imitation and innovation as well as to legal aspects of game production in general. To put it plainly, the designers, graphic artists and programmers that produce the games we play every day, and that generate enormous revenue, neither reflect legal issues in their daily work routines nor are there regular interactions with legal staff. They seem to operate with vague, lay concepts of copyright in the back of their minds. When asked directly, most developers could not assess correctly if a certain game element was protected by copyright or not, or if a certain practice crosses the line to infringement. Only in big studios are professional legal assessments included in the process, but at very late stages when production is mostly done and marketing kicks in. In sum, the regulative dimension is not totally absent from creative processes of game production, but it is certainly in the background.

B. Normative Dimension

The normative dimension addresses values and norms that classify practices as legitimate or illegitimate and appropriate or inappropriate. In contrast to the regulative dimension, rules here are neither manifest nor are they sanctioned by defined punishments. Instead, they are grounded in shared values and operate as normative expectations: “The expectations are held by other salient actors in the situation, and so are experienced by the focal actor as external pressures. Additionally, to varying degrees, they become internalized by the actor.” Typically, norms are strongly contextual and differ between communities, societies, and world regions. This dimension of governance operates according to

60. Bruce E. Boyden, Games and Other Uncopyrightable Systems, 18 GEO. MASON L. REV. 439, 479 (2011).
61. The assessment of games as objects of copyright and related IP provisions is not key to the argument of this Essay, so I keep it short. Cf. Lastowka, supra note 59, at 10; Tayebi, supra note 58; and Boyden, supra note 60 (analyzing the copyright’s application to digital games and long lists of court cases).
62. Scott, supra note 42, at 55.
In this perspective, people do not behave according to an economic calculus nor to a legal assessment, but they adjust their actions to what they perceive as appropriate in a certain situation and context.

To act appropriately is to proceed according to the institutionalized practices of a collectivity and mutual understandings of what is true, reasonable, natural, right, and good. Actors seek to fulfill the obligations and duties encapsulated in a role, an identity, and a membership in a political community. Rules are followed because they are perceived to be adequate for the task at hand and to have normative validity.

The literature on low IP regimes is strongly based on this perspective although sometimes the connection is not always drawn. The community of French chef investigated by Emmanuelle Fauchart and Eric von Hippel displays typical aspects of normative ordering. Implicit rules and shared expectations about legitimate and illegitimate practices are established, such as a prohibition of 1:1 copies, confidentiality, and referencing the original creator. Noncompliance to these expectations is not sanctioned by monetary or legal punishments but by exclusion from the community and from further sharing of expertise. With recipes and original ideas for the combination of ingredients not being protected by formal IP provisions but by these informal norms, the normative dimension and the regulative dimension are not congruent in the case of French haute cuisine.

Our interview study on game production, similarly revealed divergence between these dimensions but with a weaker normative stance and less cohesion within the community. There is consensus between professionals across the industry that “re-skinning” a game, that is plainly copying a game and only changing the art style, is an objectionable practice. Especially if the rule-based system strongly shapes the gameplay experience, copying the system and merely coating it with another visual layer is even more illegitimate.

I think it’s okay if you just copy the idea [. . .] and do your own game, your own balancing, your own pricing. What is harder or,
what I think you should not do, or what I don’t wanna do myself, is to take a game and copy it exactly, only change the art stuff.68

This informal norm runs counter to the regulative dimension, because copying the game idea and game play does not constitute copyright infringement as long as you re-program and re-skin the product.

On the other hand, the copyright infringing practice of taking art assets of classic games such as Super Mario is in many cases considered legitimate practice, as long as the game developers add interesting twists to their own game and not merely copy the whole original game.

In sum, the normative dimension rests on cohesive communities and societies to establish shared norms and expectations. The evocative cases of the low IP literature are examples of that (French chefs, U.S. comedians, magicians). In the case of the games industry, we found community norms to be less strong. This might be no surprise since the market is vast, global, and highly profitable—which rather hinders the development of shared norms. Only in the subset of so-called Indie Developers were strong community norms and beliefs recognizable.

C. Discursive Dimension

The third dimension addressed the ways we understand and talk about creative practices and products. This does not necessarily imply direct normative assessment but nonetheless shapes our thinking and doing. In Scott’s institutional theory, this dimension is denoted as the “cultural-cognitive pillar” of institutions.69 In that view, “compliance occurs in many circumstances because other types of behavior are inconceivable; routines are followed because they are taken for granted as “the way we do these things.”70 In contrast to the regulative and the normative dimension, practices here are not explicitly classified as legitimate or illegitimate. We just take certain things for granted, and routinely follow these assumptions.

Dan Burk’s paper on the sociology of patenting addresses this dimension.71 When he refers to Mircea Eliade’s definition of myths as narratives that are “true but not factual,” he exactly refers to the enduring quality and impact of widely shared beliefs that are deeply embedded in social routines and structures, so that questioning them is a hard job, even with good reasons.72

68. Material from interview study, INT17-S-M (Interviewee No. 17, S=large studio employee, M-manager).
69. SCOTT, supra note 42, at 56.
70. Id. at 58.
71. Burk, supra note 2.
72. Id. at 429; MIRCEA ELIADE, MYTH AND REALITY (1963).
In this Essay, I rename this dimension as discursive dimension, because communication and discourses are the medium in which these beliefs and frames can be identified. With “piracy” and “stealing” on the one hand, and “sharing” on the other, the copyright debates are replete with examples for discursive struggles over the ways we should understand and frame the changing practices of media and culture. While most scholarship addresses these debates only as prelude or as independent variable for the real thing, copyright reform and legislation, an institutional understanding of governance, suggests taking the discursive dimension seriously in its own right: words matter!

The brilliant works by Martha Woodmansee and Mark Rose on the emergence of the author-concept and its important impact on the consolidation of copyright as a legal instrument point to another aspect of this dimension. The regulative as well as the normative dimension are strongly dependent on the discursive dimension. Here, subjects and categories are constructed, and only on these grounds normative and regulatory provisions can operate. How do we come to privilege the author over the paper factory with regard to a book? Why do we take the idea of a self-contained work for granted, although we know that we all stand on the shoulders of giants?

With regard to our interview study, I highlight three strong currents in this dimension. The first concerns creators’ understanding of game design. All game professionals interviewed hold that game production is a highly collaborative process, full of mutual imitation and references. Devising new games always and necessarily includes great portions of existing ideas. Indeed, for a new game to become a good game, professionals argue that you should not innovate on all levels of game design; otherwise players would be confused and unable to play the game. Instead, remixing existing elements and giving the game an original twist is considered a good game design: “A lot of time it’s more about picking the right ingredients that are already there. I mean, 95% of what we do always [already] exists somewhere.”

76. Robert Baldwin et al., Understanding Regulation: Theory, Strategy, and Practice 52 (2012) (Regulatory theory has somehow included this into its concepts by acknowledging that “the underlying ideas [. . .] and the broader intellectual climate that regulat[es] instruments”—but again, are only a prelude to “serious” regulation).
77. Material from interview study, INT12-I-O (Interviewee No. 12, I-independent studio, O-owner).
The second aspect concerns game professionals’ self-concept as creatives. Almost all interviewees, whether working as independent game developers or as employees in a big studio, considered themselves as creative professionals, thus aiming for producing something new and original in their daily job. This self-concept has ramifications for the tension between imitation and innovation discussed here. Even if the management demands replicas of successful games by competitors, the developers are guided by strong intrinsic motivations to include original elements in the new game. As one interviewee put it: “I always try to smuggle something in.”

A third element in this dimension stemming from the interviews is a strong understanding of authorship in a subset of the interviewees. Indie developers articulate a strong identification with their work. They consider the developed games as “theirs,” as personal expressions. They understand the games they produce not foremost as commercial products, but as “heart projects.” Some of the indie developers who were interviewed classified their games as “Autorenspiele,” a german notion used to highlight the stronek between author and game.

D. Technological Dimension

The fourth dimension in this copyright governance model is the material-technological layer. The services and devices we use in our private and professional lives enable and at the same time, constrain the range of actions we pursue. From an institutional perspective, they contribute to ordering the social jointly with regulative, normative and discursive elements. As John Law writes, “[m]achines, architectures, clothes, texts – all contribute to the patterning of the social." In this dimension, to put it plainly, the distinction between right or wrong, and appropriate or inappropriate, is translated into possible or impossible.

In the broader field of Internet Governance, Joel Reidenberg and Lawrence Lessig made a similar argument in the late 1990s:

Law and government regulation are [. . .] not the only source of rule-making. Technological capabilities and system design choices impose rules on participants [. . .]; the set of rules for information flows imposed by technology and communication networks form a “lex informatica.”

---

78. Material from interview study, INT22-S-GA (Interviewee No. 22, S=large studio employee, GA-graphic artist).
For this perspective, Lawrence Lessig has coined the catch phrase “Code is Law.” That line of argument always runs the risk of falling into the trap of technological determinism; but if integrated into an institutional perspective, it provides an instructive impulse into our thinking about how creatives work and how products are regulated and framed.

This dimension is of particular importance for copyright research. Digital Rights Management is an obvious example for the direct delegation of regulatory functions to the technological dimension. These systems try to translate strictly the legal or illegal distinction into possible or impossible actions on our devices and services, with sometimes frustrating and bewildering results. While DRM in the pay-per-download market for music has been too inconvenient to succeed, it is today so tightly integrated into many services we use daily that we barely recognize them (e.g., streaming). Upload filtering technologies combined with IP rights databases such as YouTube’s ContentID, similarly constitute ordering processes on the technological layer. Algorithms sift through every uploaded video and identify audio snippets that match items in their IP database. As a default, every match is a potential copyright infringement, notwithstanding possible fair use practices and other restrictions of copyright claims. In effect, these systems tend to over-block content by removing works that are not infringing at all.

Turning to the case of imitation and innovation in game production, this dimension addresses the technological infrastructure of game development. Programmers and graphic artists routinely use software and programming environments that provide huge libraries and modules to help them build the game. No new game is technically built from scratch. In effect, the specific degree of imitation and innovation is strongly dependent on the technologies and their affordances. Level design, game engine, as well as control of the game character are regularly adopted from existing games—not only the concepts but also the implementation.

In sum, the technological layer is one dimension where the governance of creative production and consumption is situated. Like other institutional elements, it does not determine practices, but enables, constrains, and nudges people into one direction, and it hides alternatives.
V. A Model for Comparative Copyright Research

A. Comparing Modes of Governance Within a Sector

In analytically distinguishing different modes, discussion of their interplay sometimes gets neglected. The key analytical and empirical value of the proposed governance model is to investigate the relation between these dimensions and their respective effects. The actual relation between laws, norms, discourses, and possibly technological affordances in a specific context is an empirical question that is amenable to research.

Turning to our case study on game production, I have already highlighted several differences in the evaluation of game design practices in Part IV of this Essay. In Table 2, I summarize and compare the evaluations across the four dimensions and two practices: re-skinning and retro or homage games.

**Table 2: Comparative Evaluation of Game Design Practices**

*(Legitimate Practice and Illegitimate Practice)*

<table>
<thead>
<tr>
<th></th>
<th>Regulative</th>
<th>Normative</th>
<th>Discursive</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Skinning</td>
<td>No infringement</td>
<td>Objectionable Practice</td>
<td>Not considered creative work</td>
<td>Re-engineer the product with new code and elements</td>
</tr>
<tr>
<td>Hommage/Retro</td>
<td>Infringing use of graphics and sounds</td>
<td>If creative remake, then legitimate</td>
<td>Creative work</td>
<td>Re-use of elements</td>
</tr>
</tbody>
</table>

White box: legitimate practice; Dark box: illegitimate practice

*Re-skinning* refers to re-producing a (often successful) game by copying the logic and mechanics of a game and only changing the art style. From a legal perspective, this is in most cases a non-infringing practice. As long as graphics and sounds are substantially altered, and the software code is re-written, this does not violate copyright or other legal provisions. In contrast, the normative evaluation within the game design community strongly rejects this practice. Looking at re-skinning from the discursive perspective, this is not only considered a normatively objectionable practice, game designers more fundamentally refrain from categorizing this a creative practice in the first place. From a technological perspective, re-skinning is not effortless—all material
elements (graphics, sounds, software code) need to be redone so not to infringe upon the original.

A contrasting case is the production of hommage or retro games. Popular especially in the context of independent developers is the production of games that allude to iconic games, often from the 1980s or 1990s, such as Super Mario Brothers. Typically, game designers take the characters and maybe soundbites from these old games and produce new games with a different game-play and narrative. From a legal perspective, this regularly constitutes copyright infringement, since developers include the original, thus protected characters or very close adaption, and integrate iconic graphic elements or soundbites. Yet, from the developer community’s normative point of view, this does not violate community norms as long as the game constitutes a creative remake of the original (e.g., by performing a gender-swap of the main characters or giving the game a different twist in gameplay).

These short examples illustrate the analytical and empirical value of this model. Depending on the object of study, the four governance dimensions afford and support different creative and economic practices—and in many cases, they are not congruent. Regulative provisions diverge with normative assumptions in a community, and public discourse is at struggle with practices enabled—and maybe even nudged—by new technologies. This is not only true with game designers. The same is true for the mismatches identified by Jessica Silbey, and also for the community norms in low IP regimes. Similar to the game designers, both French chefs and comedians seem to value greatly the underlying idea of their creative works. Thus, the informal ownership claim put forward by creatives in these sectors encompasses gameplay and mechanics (game designers), the combination and preparation of ingredients (French chefs) and the core structure of a routine and joke (comedians)—elements that are typically not protected by copyright as they are considered ideas rather than works. The analytical framework presented here thus allows us to identify these mismatches and to discuss possible reactions, if necessary.


83. Id.

84. Silbey, supra note 1, at 81.
B. Comparing Modes of Governance Across Sectors

This model also allows copyright and IP scholars to compare models of governance across sectors. In the discussion of low IP regimes and other sectors, we have seen that the impact and salience of different modes of governance varies: in the case of French chef and comedians, for example, informal norms appear as the main governance mode. In game design, norms have emerged as a relevant mode as well, but regulative, discursive, and technological aspects also contribute to the ordering of creative practices. In other sectors, copyright legislation and licensing contracts might well provide for creative practices and outputs.

### TABLE 3: COMPARATIVE ASSESSMENT OF GOVERNANCE MODES ACROSS SECTORS

(STRONG IMPACT, AVERAGE IMPACT, AND WEAK IMPACT)

<table>
<thead>
<tr>
<th></th>
<th>Regulative</th>
<th>Normative</th>
<th>Discursive</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sector B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sector C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Black box: strong impact; Grey box: average impact; White box: weak impact

The schematized comparison of sectors in Table 3 illustrates the analytical value of the proposed governance model. Prevalent copyright research presumes a strong impact of law, ideally incentivizing innovation—and then concludes, allegedly with surprise, that “IP is not working as it should” or that some sectors represent a “negative space of IP.” This is because copyright researchers tend to focus on law and other legal instruments, but in the context of the presented model, this is but one dimension. In consequence, the model allows us to comparatively address the respective impact of different governance modes: regulation, norms, discourses, and technology. It turns the assumption of copyright and IP scholarship and policy (that IP has impact on creative practices

---

85. Fauchart & von Hippel, supra note 4, at 187–201.
86. Silbey, supra note 1, at 347.
87. See Rosenblatt, supra note 7.
and (b) incentivizes innovation) into an empirical question: What is the impact of IP on creative practices in relation to norms, discourses and technology? Does it hinder or promote innovation? What is considered innovation in the first place? Only by bringing different modes of governance into relation, instead of isolating regulative means, we start to fully understand the interaction between creative practices.

VI. DISCUSSION

This Essay has set out to develop a multimodal concept of copyright governance. In a nutshell, it emphasizes the point that there is always more than law in controlling IP, not only in low IP regimes. Building on institutional theories, I suggest four modes of copyright governance: (1) A regulative dimension, addressing the provision and enforcement of formal rules such as laws, court decisions, and terms of services; (2) a normative dimension, investigating the prevalent assumptions about legitimate and illegitimate behavior in a specific community or sector; (3) a discursive dimension, addressing the framings and debates on creativity, authorship, and originality; and (4) a technological dimension that investigates the embodiment of affordances and rules in infrastructures, devices, and algorithms relevant to creative work.

In analytically distinguishing different modes, discussing their interplay sometimes gets neglected. But that is exactly the core idea of this governance model—ordering takes place when these dimensions reinforce each other, but also when they contest each other. Especially in the context of copyright, divergence between these dimensions has been obvious in recent years. Technologies strongly nudge users towards infringing behaviors; norms prevalent in many communities do not fit well within the formal IP regulations.

The illustrative case study on imitation and innovation in games production similarly has shown incongruences between the dimensions. While legal regulation allows for re-skinning of games, the developers consider that a bad and objectionable practice.

The empirical value of this model is that it allows for comparative approaches. It allows comparison of the empirical impact and specific effects of the respective dimensions not only within one sector, but also across sectors. From this perspective, the prominent low IP sectors can be characterized by a low level of formal IP regulation but a high level of informal normative expectations. The governance of content on online platforms, such as YouTube or Facebook, constitutes a promising example for future case studies. On the regulative dimension, we might

88. Cf. Burk, supra note 2, at 452; Silbey, supra note 40, at 347.
expect a shift from public law to contractual elements such as Terms of Service, and Community Guidelines. Similarly, we seem to experience a shift towards regulation on the technological dimension, given the massive amount of content that these platforms host and the increasing political pressure for taking accountability for this content. As a consequence, the platforms have implemented filtering mechanisms.

I hope to stimulate the discussion on theoretical aspects of interdisciplinary copyright research with this Essay. The literature on low IP regimes has given many impulses for extending our understanding of how creative work is ordered and framed. This Essay tries to develop that line of thinking into a coherent framework that integrates diverse modes of ordering without privileging one over the other. The specific impact of the respective modes is an empirical question. I hope the copyright governance model put forward here can contribute to answering this question.
INTRODUCTION

On Tuesday, August 5, 2014, police officers in Antioch, California beat and tased a mentally ill homeless man while attempting to take him into custody.¹ Prior to police arrival, the man was reportedly dancing in

* J.D., University of Florida Levin College of Law (2017); B.A., University of Miami (2012). Tristan is a litigation attorney practicing in New York City.

¹ Carlos Miller, Northern California Cops Beat Mentally Ill Man, Seize Phones, Claim it’s their Right, PHOTOGRAPHY IS NOT A CRIME (Aug. 9, 2014), https://photographyisnotacrime.com/2014/08/northern-california-cops-beat-mentally-ill-man-seize-phones-claim-right/ (providing the perspective of a private citizen); Michael Burkholder, Opinion: TV Media Does Antioch
the street and dodging cars. According to Antioch Police, upon police arrival, they found another officer wrestling with the man, who had a magazine clip in his hands. Several witnesses to the incident assert that the man was handcuffed by police while being tased and beaten with a baton. Witnesses then observed as an officer released a K9 police dog that began to bite the man until he was bleeding and unrecognizable. After finally detaining the subject, police officers then turned their attention onto the witnesses who had recorded the incident.

Witnesses say that the officers began confiscating cellphones from anyone who had shot video of the incident using a cellular device. One witness observed as police pulled one woman out of her car and threatened to arrest her before she finally gave up her cellphone. Another witness says that he was actually ordered by police to erase the video footage from his cellphone, and described the police interactions with witnesses who initially refused to comply with police requests as “controlling” and “demanding.” Despite attempts by police, one video of the incident survived, and in it one can hear an officer of the Antioch Police Department saying he wants cameras confiscated before the video abruptly stops.

Tablets, iPads, and other forms of mobile video-recording devices have become increasingly important in modern society, and arguably none more so than cellphones. In addition to providing vital services and human connections, cellphones allow individuals to quickly share important news that often fails to make it into the daily paper or evening news broadcast. It is little wonder, then, that cellular phones continue...
to play an increasingly significant role in news production and creation, particularly at the local level.\textsuperscript{13} With the advent, rise, and current ubiquity of cellphones and other forms of mobile recording devices, instances of police brutality, particularly among minority groups, are more frequently being recorded by private citizens and broadcasted for the entire world to see.\textsuperscript{14}

Many of these mobile videos have illustrated instances of police and other law enforcement officials severely beating, brutalizing, and in many cases, shooting and killing American citizens, most of whom are either African-American or Latino and are unarmed.\textsuperscript{15} On July 5, 2016, a video was uploaded of Alton Sterling, a black male, being fatally shot after an encounter with two police officers exerting excessive force against him.\textsuperscript{16} On July 6, 2016, another video surfaced, this time of Philando Castile, also a black male, being fatally shot by police in the presence of his girlfriend and young daughter while sitting in the front seat of their car.\textsuperscript{17} These are only two instances in a long and constantly growing list of black and other minority individuals who have been brutalized and often killed by law enforcement officials. Such unfortunate and untimely deaths have only gained national attention as a direct result of witnesses recording their encounters and uploading the videos onto the internet.\textsuperscript{18}

In response to this growing trend, law enforcement officials have begun to fight this new-age vigilante news reporting by seizing and deleting cellphone video footage by these witnesses.\textsuperscript{19} But what legal authority do police officials have to seize or delete cellphone footage from private citizens? And what implications might this authority have have...
on evolving privacy interests? These are some of the questions that this paper will analyze and answer.

Part I of this Article examines cases that help illustrate the importance and need for mobile recording device footage to aid in the administration of justice. Part II discusses those constitutionally protected rights that are violated through the unlawful sequestering of a mobile video device and its footage. Finally, Part III outlines future considerations regarding the evolution of technology as it relates to the privacy interest of citizens and offers predictions as to how courts might address these issues in the future.

I. THE IMPORTANCE OF MOBILE VIDEO FOOTAGE

Part I of this Article discusses the importance of cellphone videos on society and on judicial proceedings while also highlighting the more sobering realities of the continued incorporation of this relatively new form of technology. Furthermore, Part I identifies and examines some cases where video footage displaying instances of police brutality against citizens, taken by witnesses from mobile recording devices, assisted in achieving an indictment or a conviction against those police officers responsible for the brutality.

Mobile video technology is an important tool that can be used to effectuate the true purpose and processes of the justice system. Praised by private citizens for its powerful, convenient, reliable, and indiscriminate nature; the use of mobile video technology, such as cellphones, body cameras, dash cameras, and other forms of video surveillance technology; are increasingly being used to help change the nature of policing. Improvements in technology have led to new body cameras that officers can mount onto a shirt pocket, zipper shirt, button-down shirt, or even a utility belt. By using these body cameras in tandem with the camera systems already present inside police patrol cars, police departments can improve both officer accountability and relations with the general public, whose trust in officers is currently lacking. Additionally, recent advances in cell phone technology have given civilians the power to capture their own footage by allowing them to


22. Id. at 1830, 1833 (citing David A. Harris, Picture This: Body-Worn Video Devices (Head Cams) as Tools for Ensuring Fourth Amendment Compliance by Police, 43 Tex. Tech L. Rev. 357, 360–61 (2010)).
record events—namely, police-civilian encounters—in real time. However, despite the benefits of broadcasting the proliferation of police misconduct against minorities and raising global awareness to the racial conflagration endemic in American society, this mobile technology often has little to no impact on the actual administration of justice.

Time and again, police officers who have been clearly recorded engaging in police misconduct still ultimately evade indictment and conviction. Perhaps the most infamous of such police evasion cases involves Officer Darren Wilson, a white police officer who was not indicted after he was caught on video shooting and killing Michael Brown, an unarmed black teenager in Ferguson, Missouri. Even still, should the grave reality that despite even the clearest and most veracious video evidence, most police officers escape indictment and subsequent conviction for their crimes detract from those few instances where mobile video footage was successfully used to indict and potentially convict police officers who have engaged in similar acts of brutality?

A. People v. Mehserle

Oscar Grant was only twenty-two years old when he was shot in the back at point-blank range by then-Bay Area Rapid Transit police officer Johannes Mehserle. Grant died later that day on January 1, 2009. This was after Grant and his friends, who were returning from New Year’s Eve celebrations in San Francisco, were verbally harassed with racial epithets by Mehserle and other BART police officers, who threatened to taser and kill Grant and his friends. Grant was also physically assaulted when Mehserle’s then partner, Anthony Pirone, held Grant down with both hands, and a knee on Grant’s head and neck, before Mehserle shot Grant at point-blank range in the back. Mehserle and the other officers fled the scene, then the state shortly thereafter. However, Mehserle was forced to return to California and stand trial after videos of Grant’s murder, which sparked national protests and global community outrage, went viral.

23. Id. at 1821.
24. Id.
27. Id.
28. Id.
29. Id.
30. Id.
31. Id.
According to the case file, which included witness testimony, a BART platform surveillance video, and cellphone videos taken from five BART passengers, Grant, accompanied by several friends, including his then-fiancée Sophina Mesa, boarded a train in San Francisco heading to the Fruitvale BART station. While en route, Grant became involved in a physical altercation with another passenger which quickly escalated into an all-out brawl involving at least ten men. Passengers used the train intercom to report a fight in the train’s lead car involving a large group of black males with no weapons wearing black clothing to the operator who, in turn, contacted BART central control who then contacted BART police.

Upon arrival at the Fruitvale station, the fight stopped and BART police officer Anthony Pirone spotted five African-American men, including Grant and Michael Greer, talking on the platform by the lead car. As Pirone approached, Grant and Greer got back on the train. Pirone, whom a bystander described as appearing agitated, first ordered the three men who were still standing on the platform to stand against the platform wall and keep their hands visible. Pirone then instructed his partner, Marysol Domenici, to watch the detained men against the wall.

Pirone next ordered Grant off the train and shoved him against the platform wall with the other detained men. Pirone returned to the train and ordered Greer out as well. There is conflicting testimony as to whether Greer and Grant resisted custody or failed to comply with police orders, as well as whether Pirone used offensive language or tone in his efforts to subdue them. Testimony from passengers on the train illustrate Pirone as an aggressive, hostile, and abusive, both physically and verbally. They also said Pirone used excessive or unnecessary force in his attempt to remove both Grant and Greer from the train. While Pirone used excessive force on Greer to handcuff him, Grant and the other detainees “yell[ed] at Pirone to stop what he was doing.” A passenger’s cellphone video shows Pirone hitting Grant with his fist, and witness testimony stated that Pirone shoved Grant against a wall and forced him

33. Id.
34. Id.
35. Id.
36. Id. at 2–3.
37. Id. at 3.
38. Id.
39. Id.
40. Id.
41. Id.
42. Id.
43. Id.
to his knees, after which Pirone pulled out his Taser and pointed it at the detainees, with the “taser’s red laser sight trained on Grant’s groin and chest.”

Pirone gave the order to arrest both Grant and Greer. After hearing that he was going to be arrested for resisting a police officer, Grant stood up and asked, “Who can we talk to?!” Pirone then grabbed Grant and forced him back down, with Officer Johannes Mehserle assisting by putting his hand on Grant’s head to help force him back down. Officers Domenici and Woofinden helped keep the bystanders at bay while Mehserle, Pirone, and Guerra dealt with the five detainees. Grant was kneeling on the ground while Pirone yelled racial slurs in his face. Grant fell forward onto the ground as Grant grabbed his hands from behind, and Pirone pinned Grant’s neck to the ground with his knees. Over Grant’s protestations that he surrendered, that he could not breathe, and that he was unable to move, Mehserle ordered Grant to give up his arms so he could be handcuffed and began to repeatedly pull at Grant’s right arm which was pinned underneath his body. Mehserle was heard to exclaim that he was unable to get Grant’s hands and that he was going to tase Grant.

Notably, cell phone video coverage of the melee shows Mehserle struggling to remove his handgun. When he finally retrieves it, Mehserle, holding the gun in both hands, stands and shoots Grant once in the back. Mehserle, appearing surprised and dumbfounded according to several witnesses, “holstered his handgun and put his hands on his head, then bent over and put his hands on his knees.” Grant, still conscious, shouted, “Oh, you shot me, you shot me.” Mehserle then handcuffed Grant, searched him for weapons, and discovered that Grant was not armed. Grant was taken to Highland Hospital with a single gunshot wound that penetrated his right lung, causing excessive blood loss. Grant died approximately three to four hours after his surgery.

44. Id. at 4.
45. Id.
46. Id.
47. Id.
48. Id. at 5.
49. Id.
50. Id.
51. Id.
52. Id.
53. Id.
54. Id. at 5–6.
55. Id. at 6.
56. Id.
57. Id.
58. Id.
On the platform, shortly after the shooting, Mehserle told Pirone that he thought Grant was reaching for a gun. Additionally, Mehserle talked to other officers in the minutes following the shooting and did not disclose that he had mistaken his handgun for his Taser. A still emotional Mehserle confessed later at the station to Officer Foreman that he thought Grant was going for a gun. Mehserle did not inform Officer Foreman that he thought he drew his taser instead of his handgun.

Facing a second-degree murder charge and a maximum of fourteen years in prison, Mehserle testified at his trial that he meant to draw his stun gun instead of his .40-caliber pistol. The videos taken by BART passengers were subsequently used as evidence during Mehserle’s murder trial and were also posted online, further stoking the racial tensions brought on by the shooting. Mehserle was found not guilty of murder or voluntary manslaughter, however, the jury convicted Defendant Mehserle of the lesser crime of involuntary manslaughter. Mehserle was denied probation and sentenced to two years in prison for involuntary manslaughter. Mehserle served only eleven months of his two-year sentence before he was released.

Although the outcome of Mehserle’s trial sparked nationwide outrage and protests, the spectators’ cellphone and other video footage of the struggle and Grant’s shooting was ultimately admitted as key pieces of evidence during Mehserle’s trial, which undoubtedly had a significant impact in the case. The video footage also inspired the Hollywood film, “Fruitvale Station,” which recounts the tragedy of Oscar Grant’s untimely death. This film not only helped bring awareness to Grant’s story and the experiences of minorities with law enforcement, but it also illustrated the importance of cell phone video footage and how it can be used to aid in a criminal investigation.

59. Id.
60. Id.
61. Id.
62. Id.
63. Id.
66. Id.
68. See Gahran, supra note 12.
B. State v. Van Dyke

On Monday, October 20, 2014, officer Jason Van Dyke of the Chicago Police Department shot and killed 17-year-old African-American Laquan McDonald.69 The next day, mere hours after video of him shooting McDonald was made available to the public, Van Dyke turned himself in to authorities.70 According to dashcam video footage and a criminal complaint filed in Cook County Circuit Court, the circumstances surrounding McDonald’s death began at 9:47 p.m. when Van Dyke was alerted from Cook County Police dispatch that an individual, later identified as McDonald, was being held under citizen’s arrest for allegedly breaking into trucks and stealing radio equipment.71 Minutes later, dispatch revealed that the suspect was walking away from the scene with a knife in hand.72

The dashcam video of one of the units that arrived on scene depicts McDonald as he was walking past the parked squad unit 822 patrol car.73 The video shows McDonald holding a knife as he raised his right arm.74 Van Dyke and his partner arrived on the scene and Van Dyke exited the police vehicle with his gun drawn.75 As McDonald continued to walk away from police, Van Dyke took a step towards McDonald.76 McDonald was ten feet away when he was struck by Van Dyke’s first bullets.77 McDonald fell to the floor on his side when Van Dyke fired another bullet into McDonald.78 Clouds of smoke, which were actually clouds of debris caused by the fired bullets, slowly rose from McDonald’s body.79 McDonald was still lying in the street when Van Dyke fired his last shot.80 Three more clouds of debris became visible where bullets struck the pavement close to McDonald’s body.81 As Van Dyke prepared to reload, Van Dyke’s partner could hear McDonald struggling to breathe

70. Id.
72. Id.
73. Id.
74. Id. at 3.
75. Id.
76. Id.
77. Id.
78. See id.
79. Id.
80. Id.
81. Id.
and told Van Dyke to hold his fire so that he could approach and kick the 3-inch blade away from McDonald’s body.\textsuperscript{82}

Van Dyke was armed with a 9mm semi-automatic pistol with a 16-round capacity.\textsuperscript{83} Sixteen cartridge casings were later recovered from the scene, all fired from Van Dyke’s gun.\textsuperscript{84} Analysis of video from the scene shows that McDonald was lying on the ground for thirteen of the fourteen to fifteen seconds that passed from the time Van Dyke fired his first shot to the time he fired his last shot.\textsuperscript{85} Van Dyke was also the only officer of eight on the scene that day that fired his handgun.\textsuperscript{86} After having been shot sixteen times, McDonald was pronounced dead later that evening at Mt. Sinai Hospital.\textsuperscript{87} According to the Cook County Medical Examiner, it was these multiple gunshot wounds that caused his death, making this a homicide.\textsuperscript{88}

The dashcam video of the incident does not show McDonald advancing on Van Dyke, attempting to throw his knife at Van Dyke, jumping or lunging towards Van Dyke, raising his knife as if to stab Van Dyke, or doing anything that was threatening to Van Dyke other than not responding to police commands while holding a knife, and none of the officers on scene at the time reported anything substantially different from what the video showed.\textsuperscript{89} The criminal complaint requests that “Van Dyke be held mandatory No Bail in that he personally discharged a firearm that proximately caused the death of Laquan McDonald and that a possible sentence of life imprisonment could be imposed as a consequence of his conviction.”\textsuperscript{90}

Although Van Dyke’s attorney posits a version of events where Van Dyke was actually acting in fear for his life, numbers from The Citizens Police Data Project suggest otherwise.\textsuperscript{91} The Citizens Police Data Project is a database of over 8,500 Chicago police officers that keeps record of misconduct complaints filed against each officer.\textsuperscript{92} Reports from this database revealed that Van Dyke had been the subject of a misconduct complaint on at least twenty different occasions in his fourteen-year career.\textsuperscript{93} And of those twenty, none have resulted in disciplinary action.

\begin{itemize}
\item \textsuperscript{82} Id.
\item \textsuperscript{83} Id.
\item \textsuperscript{84} Id.
\item \textsuperscript{85} Id. at 4.
\item \textsuperscript{86} Id.
\item \textsuperscript{87} Id.
\item \textsuperscript{88} Id.
\item \textsuperscript{89} Id.
\item \textsuperscript{90} Id. at 5.
\item \textsuperscript{91} See McLaughlin, supra note 69.
\item \textsuperscript{92} Id.
\item \textsuperscript{93} Id.
\end{itemize}
against Van Dyke.\footnote{Id.} Van Dyke is not alone, however, as 402 other officers in the Chicago Police Department have twenty or more complaints on file.\footnote{Id.} Van Dyke, who has since been released on $1.5 million bail, is currently awaiting trial for the first-degree murder of McDonald.\footnote{Steve Schmadeke, \textit{Prosecutors Oppose Van Dyke Skipping Routine Hearings in McDonald Case}, Ch. Trib. (Apr. 14, 2016, 5:57 PM), http://www.chicagotribune.com/news/laquanmcdonald/ct-laquan-mcdonald-jason-van-dyke-met-20160414-story.html.} Additionally, at the direction of Chicago’s police superintendent, seven of Van Dyke’s colleagues were fired for making false reports to back up Van Dyke’s story with McDonald painted as the aggressor—a story the video of the shooting proved false.\footnote{Mitch Smith & Richard A. Oppel, Jr., \textit{7 Chicago Officers Face Firing Over Laquan McDonald Cover-Up}, N.Y. Times (Aug. 18, 2016), http://www.nytimes.com/2016/08/19/us/laquan-mcdonald-chicago-police.html.} Although the fate of Van Dyke is still not certain, what remains certain is that the video footage of McDonald and Van Dyke played a significant role in helping to ensure that Van Dyke faces first-degree murder charges and that Van Dyke’s former colleagues pay for their role in Van Dyke’s crime.\footnote{Curtis Black, \textit{How Chicago tried to cover up a police execution}, Chl. Reporter (Nov. 24, 2015), http://chicagoreporter.com/how-chicago-tried-to-cover-up-a-police-execution/.}

\section*{II. The Rights of Citizens}

All people within the United States are promised and granted certain rights, as well as the protection of those rights, under both state and federal law. Part II of this Article discusses what rights, if any, are granted to private citizens as they pertain to cellphones, mobile video devices, and footage. Part II.A features some current lawsuits involving situations where private citizens have initiated federal legal proceedings against police officers and other state actors who unlawfully, and through use of coercion and intimidation, deprived them of their property and violated their constitutional rights. Section B of Part II discusses due process of law and examines how individuals, whose constitutional rights have been violated as a result of an unlawful police seizure, may bring a federal claim against their perpetrator(s). Part II.C outlines and analyzes the rights and protections granted by the First Amendment, as well as its limitations. Finally, Part II.D discusses the rights and protections granted by the Fourth Amendment, as well as its limitations.

\subsection*{A. How Mobile Video Footage is Unlawfully Sequestered by Police}

The ability of police and law enforcement officials to seize mobile video devices and footage evinces a direct implication of the protections
granted to private citizens by the First and Fourth Amendments of the U.S. Constitution. The First Amendment protects an individual’s right of free speech, while the Fourth Amendment protects an individual against unreasonable searches and seizures. These implications are further rooted in the constitutional right of due process of law granted by both the Fifth and Fourteenth Amendments. Consider the lawsuits below and note how each claim for redress is alleged under the First, Fourth, and Fourteenth Amendments, couched within a claim of a statutory violation of due process.

1. The Curious Case of Jessica Benn

On April 29, 2015, Jessica Benn attended a peaceful, anti-police brutality demonstration in Denver, Colorado with her husband. While at the demonstration, Mrs. Benn noticed as the Denver police officers at the demonstration began to arrest scores of peaceful demonstrators for no apparent reason. Mrs. Benn took out her cellphone and began to record the events occurring around her; notably, that of her husband’s face being smashed into the ground by a Denver Police officer. Police District Commander Antonio Lopez yanked Mrs. Benn’s phone away and used his baton to push her up against a bus. Commander Lopez finally released Mrs. Benn, but only after she told him that she was pregnant. Mrs. Benn never got her phone back.

Mrs. Benn filed a federal civil rights suit on March 28, 2016 against the Denver Police Commander Antonio Lopez, and the City and County of Denver, Colorado. The complaint asserts four counts against the named Defendants. Count I asserts that Plaintiff’s act of recording the police officers’ actions in public constituted protected speech, expression, and news-gathering under the First Amendment, and that Lopez—acting within the scope of his employment—violated Mrs.

100. U.S. CONST. amend. IV.
103. Id.
104. Id.
105. Id.
106. Id.
107. Id.
109. Id. at 14–15.
Benn’s First Amendment rights in direct retaliation to her exercise of those rights.110

Count II of the lawsuit makes a claim under 42 U.S.C. § 1983 as it pertains to the Fourth Amendment, alleging a violation of Mrs. Benn’s right against unreasonable searches and seizures. Count III of the complaint asserts a claim under 42 U.S.C. § 1983 as it pertains to the Fourteenth Amendment, and alleges a violation of Mrs. Benn’s due process of law when Lopez permanently deprived her of her cell phone. Finally, Count IV of the complaint makes a claim of indemnification under Colorado state law, and asserts that the City of Denver is responsible for paying any compensatory damages, as Lopez was an employee of the City and County of Denver and was acting within the scope of his employment when he accosted Mrs. Benn.111

2. The Lengthy Lawsuit of Levi Frasier

On August 14, 2014, Levi Frasier witnessed two men pull another young man out of his vehicle.112 Frasier immediately took out his tablet and began recording.113 The “two men” Frasier initially identified happened to have been two Denver police officers.114 The officers continued trying to restrain the suspect, who was already on the ground, as they attempted to get the suspect to give up the plastic bag he had just placed in his mouth.115 After yelling to the suspect to spit out the drugs, one of the officers became enraged by the suspect’s lack of compliance and began to punch the suspect repeatedly in the face, as the suspect lay there on the ground.116 As the suspect’s pregnant girlfriend approached the officers, one of the officers reached out and grabbed her leg. There were screams, and the pregnant woman fell to the ground.117

Still recording on his tablet, one of the officers finally noticed Frasier and yelled, “Camera!”118 An officer later asked Frasier for the video.119 Frasier, unwilling to give up the video, first told the officer that he had

110. Id.
111. Id.
113. Id.
114. Id.
115. Id.
116. Id.
117. Id.
118. Id.
119. Id.
only taken a picture. He then told the officer that he had taken the video with his cell phone and not the tablet. By this time, several officers had begun to surround Frasier, who was beginning to feel intimidated and coerced. The officers asked Frasier again whether he was going to give them the video; he responded that he would not do so without a warrant. At this time, one of the officers simply took Frasier’s tablet. After about four minutes, the officer returned the tablet to Frasier. However, the video recording Frasier had just taken only moments earlier was now gone.

The next day, Frasier filed a federal civil lawsuit against Officers Christopher Evans, Charles C. Jones, John H. Bauer, Russell Bothwell, as yet unidentified Denver police officers, and the City and County of Denver, Colorado. The complaint outlines eight counts against the named Defendants, including a violation of the Plaintiff’s First, Fourth, and Fourteenth Amendment rights.

B. 42 U.S.C. § 1983 and Due Process of Law

The Fifth Amendment and the Fourteenth Amendment of the U.S. Constitution prohibit governmental deprivations of “life, liberty, or property, without due process of law.” However, an analysis of the Fourteenth Amendment must begin with an analysis of the Fifth Amendment, as much of the language of the Fourteenth Amendment is drawn directly from the Fifth.

1. The Due Process Clause of the Fifth Amendment

Similar to the Fourteenth Amendment, the Fifth Amendment of the United States Constitution provides, in relevant part: “No person shall . . . be deprived of life, liberty, or property, without due process of law.”

120. Id.
121. Id.
122. Id.
123. Id.
124. Id.
125. Id.
126. Id.
128. Id. at 11–21.
129. U.S. CONST. amend. V.
130. See Ely, supra note 101.
131. U.S. CONST. amend. V.
The court in *Hurtado v. California* established a test to determine what constitutes “due process of law” under the Fifth Amendment132: “that any proceeding otherwise authorized by law, which is not thus sanctioned by usage, or which supersedes and displaces one that is, cannot be regarded as due process of law.” The court further acknowledges:

A State cannot deprive a person of his property without due process of law; but this does not necessarily imply that all trials in the State courts affecting the property of persons must be by jury. This requirement of the Constitution is met if the trial is had according to the settled course of judicial proceedings. Due process of law is process according to the law of the land. This process in the States is regulated by the law of State.133

Ultimately, the court held that “any legal proceeding enforced by public authority, whether sanctioned by age and custom, or newly devised in the discretion of the legislative power, in furtherance of the general public good, which regards and preserves these principles of liberty and justice, must be held to be due process of law.”134

The core meaning of “law of the land” provisions, dating back to the Magna Carta, is to secure the principle of legality by ensuring that executive and judicial deprivations are grounded in valid legal authority.135 In this respect, the Fifth Amendment's Due Process Clause limits the substance of executive or judicial action by requiring it to be grounded in law.136

2. The Due Process Clause of the Fourteenth Amendment

As a constitutional doctrine, the Due Process Clause of the Fourteenth Amendment serves three separate functions.137 The Fourteenth Amendment provides, in relevant part138:

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without

---

133. *Id.* at 533.
134. *Id.* at 537.
136. *See id.*
due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

The U.S. Supreme Court explains in Daniels v. Williams the three different types of constitutional protections that are granted by the Fourteenth Amendment, ultimately broadening the scope of due process law. As outlined by the court in Daniels:

First, it incorporates specific protections defined in the Bill of Rights. Thus, the State, as well as the Federal Government, must comply with the commands in the First and Eighth Amendments; so too, the State must respect the guarantees in the Fourth, Fifth, and Sixth Amendments. Second, it contains a substantive component, sometimes referred to as “substantive due process,” which bars certain arbitrary government actions “regardless of the fairness of the procedures used to implement them.” Third, it is a guarantee of fair procedure, sometimes referred to as “procedural due process”: The State may not execute, imprison, or fine a defendant without giving him a fair trial, nor may it take property without providing appropriate procedural safeguards.139

Under the modern law interpretation, both the federal and state governments are subject to the same substantive and procedural due process rights under the Fifth and Fourteenth Amendments.140 Thus, an individual may make a Fourteenth Amendment due process claim under either of these three categories.

However, a claim under the first or second category (a direct violation of the Bill of Rights or a substantive due process claim) first requires a violation of 42 U.S.C. § 1983, which provides civil action for the deprivation of rights.141 42 U.S.C. § 1983 reads:

 Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a

139. Id.
140. Ely, supra note 101.
141. See Daniels, 474 U.S. at 338.
declaratory decree was violated or declaratory relief was unavailable.142

The court in Daniels analyzes each of the three categories of a Fourteenth Amendment due process claim. Under both the first and second categories, a plaintiff may invoke § 1983 regardless of the availability of a state remedy.143 However, claims under the third category are described as follows:

A claim in the third category—procedural due process claim—is fundamentally different. In such a case, the deprivation may be entirely legitimate—a State may have every right to discharge a teacher or punish a student—but the State may nevertheless violate the Constitution by failing to provide appropriate procedural safeguards . . . In a procedural due process claim, it is not the deprivation of property or liberty that is unconstitutional; it is the deprivation of property or liberty without due process of law—without adequate procedures.144

Most provisions of the Bill of Rights are applicable to both the state and federal governments in the exact same manner. Thus, the fundamental difference between a substantive due process claim and a procedural due process claim is that a substantive due process claim requires an illegitimate deprivation of rights or property, whereas a procedural due process claim goes two steps further. In a procedural due process claim, not only can the deprivation be either legitimate or illegitimate, but the deprivation must also be one that deprives the individual of fair and adequate procedure—a trial, legal proceeding, tribunal, or other State remedy. Specifically, unless there is some legitimacy in the seizure, a person’s personal property cannot be taken away from that person by any individual or by the State without that person being granted the opportunity to be heard before a tribunal (e.g., court, trial, legal proceeding).

3. Applying the Fourteenth Amendment to Cellphones

A personal cellphone constitutes one’s personal property in which, under the Fourteenth Amendment, that individual has protection through property rights. However, the law also provides exceptions to this blanket protection of rights. The law denies individuals’ property rights in illegal drugs and other contraband, which could also be classified as one’s

143. Daniels, 474 U.S. at 337–38.
144. Id.
The law also denies individual rights in commonplace items that are used in illegal ways. Applying this to cellphones, it is arguable that one’s property rights in his or her cellphone may be stripped if it is determined that the he or she has used the phone to further illegal conduct, such as using the phone to aid in the trafficking of illegal drugs or videotaping child pornography. However, the mere act of using one’s cellphone to record police officers engaging in brutal behavior against citizens is not, in and of itself, unlawful or considered a prohibited use as to strip away one’s property rights in their cellphone or its footage.

C. Freedom of Speech and the First Amendment

The First Amendment of the U.S. Constitution provides that, “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” The relevant portion of this clause as it pertains to the issue raised in this paper is the prohibition on the freedom of speech, a freedom granted to all people of the United States. The freedom of speech is, in fact, quite broad and rather generous, as it allows individuals the right to engage in a myriad of activities, including: the right of symbolic speech, the right to advertise commercial products and professional services, the right to contribute money to political campaigns, the right to use offensive words and phrases to convey a political message, and it also allows all people, even Colin Kaepernick, the right not to speak, not to salute the flag, and not to stand and place their hands over their hearts during the national anthem.

This right also extends to recording video and audio of police using a cellphone, tablet, iPad, camcorder, or any other type of mobile video recording device. Under the First Amendment, all people of the United States have the right to record the police because public servants

146. 21 U.S.C. § 881(a)(4), (h) (2012); see Nelson, supra note 145.
147. U.S. CONST. amend. I.
performing their public duties in a public place have no right to privacy regarding a citizen’s right to record their actions.\textsuperscript{153} Courts have ruled that “[r]ecording governmental officers engaged in public duties is a form of speech through which private individuals may gather and disseminate information of public concern, including the conduct of law enforcement officers.”\textsuperscript{154}

Although broad, the freedom of speech granted under the First Amendment is not to be construed as a “blanket” protection, as it is accompanied by some limitations. There exists “time, place and manner” restrictions on filming.\textsuperscript{155} Individuals are not granted the right to demand access to a location from which citizens can gather information.\textsuperscript{156} The court in \textit{Houchins v. KQED} denied a broadcasting company access to a particular location of a county jail that had alleged abusive conditions and that had also been the site of a recent inmate suicide, holding that, “there is no basis for the claim that the First Amendment compels others—private persons or governments—to supply information.”\textsuperscript{157} Individuals are also not granted the right to gather news by any means they think necessary.\textsuperscript{158} In \textit{Branzburg v. Hayes}, a group of journalists claimed that compelling them to testify about confidential sources would violate their First Amendment right to gather news, and the court held that the First Amendment “does not invalidate every incidental burdening of the press that may result from the enforcement of civil or criminal statutes of general applicability.”\textsuperscript{159} Although individuals are granted the right to access criminal trials under \textit{Richmond Newspapers v. Virginia} (which held that the First Amendment provides the public with a constitutional right of access to criminal trials because they historically had been open to the public and because “it would be difficult to single out any aspect of government of higher concern and importance to the people . . . .”),\textsuperscript{160} recent case law has declined to extend the right of this access beyond the courtroom.\textsuperscript{161} In \textit{Los Angeles Police Dep’t v. United Reporting Publishing Co.}, the court upheld a California law denying access to arrestees’ addresses if the request was made for commercial purposes, 

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{153} Glik v. Cunniffe, 655 F.3d 78, 82 (1st Cir. 2011).
\item \textsuperscript{154} Id.
\item \textsuperscript{155} Id. at 84.
\item \textsuperscript{156} Houchins v. KQED, Inc., 438 U.S. 1, 11 (1978); see Cornelius v. NAACP, 473 U.S. 788, 799–800 (1985).
\item \textsuperscript{157} Houchins, 438 U.S. at 11.
\item \textsuperscript{158} Branzburg v. Hayes, 408 U.S. 665, 682 (1972).
\item \textsuperscript{159} Id.
\item \textsuperscript{160} Richmond Newspapers v. Va., 448 U.S. 555, 575 (1980); see Globe Newspaper Co. v. Superior Court of Norfolk, 457 U.S. 596 (1982).
\item \textsuperscript{161} L.A. Police Dep’t v. United Reporting Publ’g Corp., 528 U.S. 32, 40 (1999); see also Estes v. Texas, 381 U.S. 532 (1965) (holding that excessive televising and broadcasting of criminal trial was a violation of due process).
\end{itemize}
\end{footnotesize}
stating that the law represented “nothing more than a governmental denial of access to information in its possession.”

As it specifically concerns the filming of police officers by private citizens, a person’s right to record police is limited only by the usual “reasonable time, place, and manner restrictions” which can be placed on acts protected by the First Amendment. The Supreme Court has recognized that the government has a significant interest in protecting safety and has upheld speech restrictions grounded in safety concerns against First Amendment challenges. While cellphones and cellphone cameras are not inherently dangerous, their use can undoubtedly create safety hazards. Such restrictions on one’s right to record might include citizen-recorders coming too close or approaching police from behind or oblique angles, posing a risk to officers looking to minimize their own vulnerabilities as well as those of members of the public; recording police officers while knowingly trespassing in order to obtain footage; ordering a person to step back or to record from a distance where a suspect might have a gun or dangerous weapon; or creating a situation where a person’s actions are clearly causing serious interference with the police investigation. Given these examples, the issue of safety remains the cornerstone of such restrictions on police recording, as police officers must be able to protect and maintain their own safety as well as that of the public.

However, police are prohibited from using a “time, place and manner” restriction to justify a refusal to allow an individual to film what is in plain sight if the officer’s purpose is to impose a “content-based restriction,” that is, to censor what is being recorded. For example, police are not permitted to interfere with parents filming their children’s piano recital at a school or filming their children’s football game at a public park.

There are some circumstances where police can justify a content-based restriction. The police may block off the area in which offenders

162. United Reporting Publ’g, 528 U.S. at 40.
165. Regan, supra note 163.
168. Id.
have taken a hostage in order to prevent someone from broadcasting police efforts to free the hostage or to preserve the hostage’s privacy.\textsuperscript{170} However, in each of these cases, there is a compelling government interest—usually to prevent ordinary citizens from unwittingly interfering with police efforts.\textsuperscript{171} However, this compelling interest should not be used to prevent the free flow of accurate and credible news, and it should never be used to protect officers who, after having been caught on video engaging in misconduct, may not be viewed in the most favorable light.\textsuperscript{172}

D. Privacy Interests and the Fourth Amendment

The Fourth Amendment grants protection against unreasonable searches or seizures by state actors, such as police. The Amendment reads\textsuperscript{173}:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Cellphones are considered “effects” which fall under the protection of the Fourth Amendment.\textsuperscript{174} Also, as previously discussed, the data stored within a person’s cellphone, including audio and video footage, must be held distinct and separate from the actual phone itself, as a digital video or audio recording is not a tangible device.

1. The Riley Court and the Development of Privacy Interests

The Supreme Court of the United States examined two separate cases in \textit{Riley v. California}, using both to outline what interest, if any, an individual has in the digital contents of their cellphone.\textsuperscript{175} In the first case, petitioner David Riley was convicted and given a higher sentence after police searched his phone and found evidence that Riley may have been involved in gang-related activity.\textsuperscript{176} In the second case, respondent Brima

\begin{itemize}
\item \textsuperscript{170} Id.\textsuperscript{170}
\item \textsuperscript{171} Bernick Larkin, \textit{supra} note 167.\textsuperscript{171}
\item \textsuperscript{172} Id.\textsuperscript{172}
\item \textsuperscript{173} U.S. CONST. amend. IV.\textsuperscript{173}
\item \textsuperscript{174} See Maureen E. Brady, \textit{The Lost “Effects” of the Fourth Amendment: Giving Personal Property Due Protection}, 125 YALE L.J. 946, 1003 (2016).\textsuperscript{174}
\item \textsuperscript{175} Riley v. California, 134 S. Ct. 2473, 2480 (2014).\textsuperscript{175}
\item \textsuperscript{176} Id. at 2481.\textsuperscript{176}
\end{itemize}
Wurie was charged with drug and firearm offenses when, after being arrested in an apparent drug sale, police officers seized a cellphone from Wurie’s person and searched through the recent call logs. From the call logs, they were to trace a frequently-appearing number to Wurie’s apartment where they found drugs, a firearm, and ammunition.

Three related precedents govern the extent to which officers may search property found on or near an arrestee. The court in *Chimel v. California* required that a search incident to arrest be limited to weapons and evidence within the arrestee’s immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction. Applying the *Chimel* analysis in *United States v. Robinson*, the court held that the risks identified in *Chimel* are present in all custodial arrests, even when there is no specific concern about the loss of evidence or the threat to officers in a particular case. Finally, *Arizona v. Gant* permits searches of a car where “the arrestee is unsecured and within reaching distance of the passenger compartment,” or where “it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle.”

The court in *Riley* refused to extend the categorical rule from *Robinson* to searches of data stored on cellphones. The *Riley* court further refused to import the *Gant* standard from the vehicle context to allow a warrantless search of an arrestee’s cellphone whenever it is reasonable to believe that the phone contains evidence of the crime giving rise to arrest. In reaching its decision, the court in *Riley* ultimately looked to *Chimel*, which arguably laid the groundwork for modern-day privacy interest analyses. *Chimel* opined that there are two overarching interests that must be served when dealing with searches of private property by police officers: (1) seizure of items that could be used to harm an officer or escape; and (2) destruction of evidence.

Using *Chimel* as a baseline, *Riley* addressed each issue raised by the *Chimel* court and determined that, as to the first issue, the digital data stored on a person’s cell phone is not a ‘weapon’ in the traditional sense, in that it cannot cause physical harm to an arresting officer or assist an arrestee in escaping. Police officers are allowed to examine the

177. *Id.*
178. *Id.*
179. *Id.* at 2483.
182. *Id.* at 2484 (citing *Arizona v. Gant*, 556 U.S. 332, 343 (2009)).
183. *Id.* at 2485.
184. *Id.* at 2492.
185. *Id.* at 2488–89.
187. See *Riley*, 134 S. Ct. at 2485.
physical aspects of the phone to identify whether there is anything hidden within it that might be used as a weapon, like a razor blade, but the data on the phone does not pose a danger to anyone. In addressing the second issue raised in *Chimel*, the *Riley* court observed that there was a legitimate concern regarding the issues of remote wiping and data encryption of the digital data stored on phones. However, the court concluded that not only is neither issue truly prevalent, but that there are also other avenues by which an officer can address the unlikely problems of remote wiping, data encryption, and the untimely destruction of relevant digital information stored within a cellphone. In short, the court ultimately held that, due to the proliferation of cellphone use as well as the sheer volume of data and storage capacity that cellphones contain, there exists a legitimate and extensive privacy interest in the digital contents of cellphones. As such, police generally may not, without a warrant, search digital information on a cellphone seized from an individual who has been arrested.

2. Reasonable Expectations of Privacy

In determining whether a Fourth Amendment constitutional violation has occurred, most courts also apply the standard Fourth Amendment test: whether the government has violated the claimant’s “reasonable expectation of privacy.” Inspired by the Fourth Amendment, case law has further developed this idea by dividing this concept into two similar yet distinct entities: the subjective reasonable expectation of privacy and the objective reasonable expectations of privacy, both approaches requiring a two-fold inquiry.

*Katz v. United States* discusses what constitutes a subjective expectation of privacy. The court in *Katz* states:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’ Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities,

---

188. *Id.*
189. *Id.* at 2486.
190. *Id.* at 2486–87.
191. *Id.* at 2494–95.
192. *Id.* at 2495.
or statements that he exposes to the “plain view” of outsiders are not “protected” because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.196

Thus, a subjective expectation of privacy would be one where the individual who is seeking protection has a legitimate, personal expectation of privacy; that is, an expectation of privacy that the individual himself would reasonably expect to have.197

Similarly, the court in *Dow Chem. Co. v. United States* argues as to what an objective expectation of privacy standard is.198 Although the two-pronged analysis is generally the same for both standards, an objective expectation of privacy analysis requires there to be an actual (objective) expectation of privacy.199 The court in *Dow* reasoned, “Dow plainly has a reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings, and it is equally clear that expectation is one society is prepared to observe.”200 Thus, an objective expectation of privacy standard requires an individual to have a reasonable and legitimate expectation of privacy that society would also view as being a reasonable and legitimate expectation.201 For example, as it relates to expectations of privacy regarding information, an expectation of privacy in information that is concealed would be more objectively reasonable than a subjective expectation of privacy in information that is exposed. Also, a person engaging in activity within the confines of her home with the doors closed and the blinds drawn would have a more objectively reasonable expectation of privacy than someone engaging in activity in a public place, where even a subjective expectation of privacy is only arguable, at best.

III. Future Considerations and Predictions

Looking forward, it is important to note that an individual’s privacy interest is not a fixed and immutable section of law. Rather, it is a concept that continues to be affected and shaped by changing ideas, values, and perceptions. The right of protection of one’s privacy will continue to be extended so long as individuals assert their claims over what they deem to be private. As technology advances and society continues to change,
those protections will likely become increasingly restrictive. Part III.A
discusses the role and potential impacts of advances in technology on
future Fourth Amendment analyses and individuals, particularly police
officers. Part III.B addresses the potential impact that continued
widespread dissemination of mobile video footage and other personal
information may have on people and future court decisions surrounding
the issue of privacy rights and reasonable expectations of privacy.

A. Implications of Technological Advances

Technology continues to develop and advance at a breathtaking pace.
Undoubtedly, the effects of such high-speed technological development
have been majorly positive. Not only do advances in technology allow
people to live longer, healthier lives, but these advancements have also
sparked waves of innovation, creativity, and ingenuity; challenging each
consecutive generation to go further, to do more, and to be better than
their predecessors. Most recently, at the Davos World Economic
Forum, world leaders and innovators were surveyed in regards to what
upcoming technological advances and futuristic capabilities may be in
the works. One such technological advance that was mentioned was
the capability of implanting a phone inside a person’s head.

Although creative and socially relevant in its own right, talk of this
new technological capability begs the question as to whether anyone has
taken pause to seriously analyze the legal implications of such an
endeavor. As discussed earlier, there are exceptions to when an officer
may request and seize and individual’s cellphone footage. If taking and
storing mobile videos became as easy as blinking an eye, how would
police go about lawfully seizing that person’s footage? If phones were to
be implanted inside a person’s head, where would the data go? And how
would such data be transferred from person to person? More importantly,
how would that data be erased? Remote wiping, which was previously
held to not be prevalent or a legitimate concern for police officers,
would soon undoubtedly become increasingly legitimate and highly
prevalent. The continued development of technological advances would

b_2545273.html.

203. Tomas Chamorro-Premuzic, Is Technology Making Us More Creative?, GUARDIAN
(June 18, 2015, 5:00 AM), https://www.theguardian.com/media-network/2015/jun/18/
technology-creative-creativity-web-content.

204. Marguerite Reardon, The Mobile Phone of the Future Will Be Implanted in Your Head,
CNET (Jan. 19, 2016, 4:00 PM), https://www.cnet.com/news/the-mobile-phone-of-the-future-
will-be-implanted-in-your-head/.

205. Id.

206. Riley, 134 S. Ct. at 2487.
ultimately create a significant concern more so for police than for private citizens, as acts once deemed too difficult or impossible to ever truly be a legitimate cause for concern might soon become very possible.

B. Implications of Widespread Dissemination

Privacy rights will also play a large role in shaping future legislation surrounding this and similar issues. One major source of concern in this area involves the expectation of privacy. A person has certain expectations of privacy in various kinds of property. As to cellphone video footage and data stored within a cellphone, it has been established that there exists an objectively reasonable expectation of privacy. But how far will future courts go in protecting a person’s privacy interests when they are freely given away?

In today’s society, simply taking and storing a video is no longer enough; it must be shared with the entire world. When a video is recorded using someone’s cellphone and then disseminated on the internet, it becomes global information. What objective, or even subjective, reasonable expectation of privacy does one have in a video that has been broadcasted over the internet for the entire world to see? Similarly, what expectation of privacy does a person have in a video of police engaging in misconduct after that video has been posted to Facebook? Would it then be unreasonable or unlawful for the officer to then seize the phone for its “content”? In the interest of fairness, some courts would likely begin deciding that people no longer have any reasonable expectation of privacy in any data stored on their phones, as it is already given away so freely.

CONCLUSION

Absent a validly-served warrant, the sequestering of cellphone video footage by police officers is, in most cases, unlawful, illegal, and wrong. The U.S. Constitution grants the People protection from unwarranted government intrusion, which includes unreasonable searches and seizures. Aside from a few limitations, a person is well within her legal right under the First Amendment to record any police officer engaging in misconduct in a public place. Any efforts to prevent a person from doing so is a clear violation of that person’s First Amendment rights. People should also not be mistreated, coerced, or intimidated by police to relinquish their personal property or delete its contents. Any such coercion is a violation of that person’s Fourth Amendment right.

207. Id. at 2494–95.
Unfortunately, due to institutional racism and failures of the judicial system, video recordings of police engaging in misconduct many times have little to no impact on the offending officer. More weight and attention must be given to video-recorded footage, as it is one of the most indiscriminate and reliable forms of evidence available today. There will be no change to the status quo if officers, emboldened by a false sense of invincibility, continue to escape conviction or judicial discipline for their blatant misconduct. Nevertheless, regardless of what little impact a video recording may have on the actual adjudication of justice against an offending officer, the benefits of recording still outweigh the courts’ failure to take recordings into consideration.

Courts must have a clear and accurate account of events as they occurred in order to properly process excessive force claims under 42 U.S.C. § 1983. Not surprisingly, one of the best ways for courts to do this is through civilian footage of police-civilian encounters. This type of footage also serves to disincentivize officers who may be otherwise tempted to lie under oath, either to protect themselves or their colleagues. Knowing that there is tangible, verifiable proof of what actually occurred during an event is sure to deter many officers from blatantly lying in any statement or tribunal. Footage of police brutality and misconduct, especially recordings involving minority victims, should continue to be filmed and broadcasted to incite people to action and to galvanize grassroots coalitions that will advocate for judicial reform as well as a dismantling and rebuilding of the current broken system.

As quickly as society continues to develop, courts too should develop. The momentum of the rise of new technological advances will likely overtake the slow, inconsistent march of the courts, and legislation will soon fall below the curve. Future generations of attorneys and lawmakers, born and bred in this age of technological revolution and wonder, are perfectly primed to assist the courts in picking up the pace. As the intersectionality of law and creative technology continues to become more readily apparent, institutions of higher learning and legal education should also begin to refocus and restructure their ancient, decrepit curriculums and stale practices in order to adapt to the increasingly changing legal landscape. Law, like technology, should constantly be looking forward, and seldom backwards. As with all things, the law, its teaching, and its application must continue to advance and adapt or it will eventually decay and die.

208. See Nunes, supra note 21, at 1842.
209. Id.
210. Id.
211. Id.
A CASE AGAINST BAD MATH

Peggy Bruner*

INTRODUCTION

If you google1 any of one your favorite Tech News blogs, you will likely see at least one of the following phrases on the homepage: “artificial intelligence,” “machine learning,” or “algorithm.” An algorithm, the basis of this fast-growing area of computer science, is a sequence of instructions telling a computer what to do.2 Machine learning uses algorithms to “learn” by “minimizing error or maximizing the

* J.D., University of Florida Levin College of Law; B.A. 2015, Auburn University. I would like to thank my friends and family for their constant support. I would also like to thank Adam Curry and John C. Dvorak of the No Agenda Podcast for drawing my attention to this important topic. Lastly, thank you to all of the members of the Journal of Technology Law and Policy for their hard work and dedication.


likelihood of their predictions becoming true.” Artificial Intelligence uses algorithms to perform tasks that would otherwise require human behavior, such as visual or audio recognition. Over the last few years, big data companies like Netflix, Amazon, and Facebook have introduced algorithms to suggest movies you might like, products you might want to purchase, or people you may know based on the inputs you give each algorithm.

I. THE PROBLEM WITH ALGORITHMS

I never would have guessed that this type of math was responsible for advancing systemic discrimination until I watched a TED Talk by Cathy O’Neil. O’Neil explained how algorithms are used by big data companies to determine who fills an open job position, who gets an interview, or who pays more for their insurance. She highlighted how the public does not get to see the magic formulas that make these decisions. Cathy O’Neil has been investigating these secret formulas and dedicated the last few years writing a book about them. In her cleverly titled book, Weapons of Math Destruction, she explains the problems with these secret formulas and our inability to question and change them. Throughout her book and speeches, she makes a call for action, asking society to accept fairness over accuracy.

O’Neil describes how this type of discrimination, hidden deep in source code, is typically invisible to the public. Just because discrimination is hidden does not mean it is insignificant. Often times, this type of discrimination is illegal. In other situations, biased algorithms perpetuate negative and harmful stereotypes. For example, a study in 2013 found that Google’s results for searches of common African-American names would often show suggestions that the person had an arrest record, even if he or she did not. Many people might not

4. Id.
6. Id.
7. Id.
9. Id.
initially understand the implications of an individual’s negative Google search results. Therefore, imagine applying for a job where the employer’s first step in a background check is to search the individual’s name on an online search engine such as Google. When pages of results are suggestions for another similarly named individual’s potential arrest records, an employer is likely to end his or her preliminary background check, and potentially the individual’s application process altogether.

This problem has been detected, investigated, and reported many times over several years. Corporations and government organizations have exponentially continued, however, to develop new algorithms. Our institutions place blind faith in mathematical formulas, hoping for maximized efficiency and profits.

II. LEGAL APPROACHES TO INVESTIGATING DISCRIMINATORY ALGORITHMS

The success of O’Neil’s speech and book has shone a light on insidious discrimination hidden deep inside mathematical formulas that falsely appear objective. The public’s demand to hold big data companies accountable is critical to finding and fighting bias deep within the source code. Legally speaking, computer scientists, academic researchers, and journalists face many hurdles when investigating this problem. The criminal justice system continues to use software to predict the likelihood that a criminal will commit a crime in the future, despite vast research showing the software makes racially discriminatory assumptions. On the consumer protection front, researchers have identified discriminatory business practices and successfully pressured corporations into changing those practices. But a suit filed by the ACLU on behalf of researchers investigating potential housing and employment discrimination online shows there are additional legal hurdles researchers have to overcome when tackling algorithmic discrimination.12

A. Algorithms in the Criminal Justice System

The criminal justice system uses algorithms in crime prediction software and “risk assessment” tools.13 Crime prediction software programs, like PredPol, CompStat, and HunchLab, are software programs that process past data to predict where crimes are likely to occur.14 Police departments benefit from these programs when faced with

14. O’NEIL, supra note 8, at 85.
substantial financial restraints and a limited number of officers available for patrolling a given community.  

Risk assessment software is employed to predict a defendant’s recidivism rate, or the likelihood a defendant will commit a crime again; it’s used to set bail and determine sentences. This software uses algorithms to calculate risk based on factors such as a defendant’s age, sex, location, family background, and employment. One example of this software is the Level of Service Inventory-Revised (LSI-R), which is a quantitative survey of offender attributes and their situations relevant to the level of supervision and treatment decisions. The LSI–R helps predict parole outcomes, success in correctional halfway houses, institutional misconducts, and recidivism. 

Another example of risk assessment software is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), which is used for decisional support in the Department of Corrections when making placement decisions, managing offenders, and planning treatment. COMPAS uses information gathered from a defendant’s criminal file and an interview with the defendant to produce a report that consists of predicted recidivism and potential needs related to substance abuse, housing, and employment. The COMPAS assessment calculates pre-trial, general, and violent recidivism risks on a one to ten scale. COMPAS predicts the general likelihood that a criminal is either more or less likely to commit another crime following release from custody based on those with a similar history of offending.

1. State v. Loomis

The Wisconsin Supreme Court reviewed the constitutionality of the algorithm used by COMPAS in State v. Loomis. Loomis was the driver in a drive-by shooting. He was charged with five counts, including first-degree recklessly endangering safety, operating a motor vehicle without the owner’s consent, attempting to flee a traffic officer, possession of a firearm by a felon, and possession of a short-barreled shotgun or rifle.
Loomis denied any involvement with the crime, and pleaded to two of the less severe charges: attempting to flee a traffic officer and operating a motor vehicle without the owner’s consent. The plea agreement dismissed the other counts but included the following:

The other counts will be dismissed and read in for sentencing, although the defendant denies he had any role in the shooting, and only drove the car after the shooting occurred. The State believes he was the driver of the car when the shooting happened. The State will leave any appropriate sentence to the court’s discretion, but will argue aggravating and mitigating factors.

After Loomis accepted the plea, he was subjected to a presentence investigation which included a COMPAS risk assessment. The COMPAS scores predicted that Loomis was highly likely to commit another crime before trial, another crime in general, and a violent crime. Although the COMPAS report stated that its scores “should not be used to determine the severity of the sentence or whether the offender is incarcerated,” the State argued that the court should consider the report in determining Loomis’s sentence. The court used the COMPAS scores among other factors in excluding the possibility of probation. The court sentenced Loomis to six years in prison and five years of supervised parole. After sentencing, Loomis filed a motion for post-conviction relief requesting a new sentencing hearing, alleging the court’s use of the COMPAS risk assessment violated his due process rights.

At the due process hearing, expert witness Dr. David Thompson testified for the defense, explaining that the court’s consideration of the COMPAS risk assessment runs a serious risk of overestimating an individual’s risk. Dr. Thompson also pointed out how little information courts have about how the COMPAS software analyzes the recidivism risks of each defendant; he stated, “[t]he Court does not know how the COMPAS compares that individual’s history with the population that it’s comparing them with. The Court doesn’t even know whether that population is a Wisconsin population.” The court denied the post-conviction motion, explaining that it used the COMPAS report to

27. Id.
28. Id.
29. Id.
30. Id. at 755.
31. Id.
32. Id.
33. Id. at 756 n.18.
34. Id. at 756.
35. Id.
36. Id. at 756.
corroborate its findings and that it would have imposed the same sentence regardless.\textsuperscript{37}

On appeal, the court considered whether the circuit court’s consideration of the COMPAS risk assessment report violated Loomis’s constitutional right to due process as a question of law.\textsuperscript{38} The court found that a sentencing court may consider a COMPAS risk assessment report at sentencing but not to incarcerate an offender or to determine the severity of the sentence.\textsuperscript{39} The court restricted the use of the report, holding that it “may not be considered as the determinative factor in deciding whether an offender can be supervised safely and effectively in the community.”\textsuperscript{40}

2. ProPublica’s Algorithm Audit

In May 2016, ProPublica released a report on a number of states and their use of the COMPAS recidivism algorithm.\textsuperscript{41} As a part of the report, ProPublica studied 10,000 criminal defendants in Broward County, Florida and compared their predicted recidivism to their actual rates over a two-year period.\textsuperscript{42} They found that African-American defendants were predicted to be riskier than they actually were, and white defendants less risky than they were.\textsuperscript{43} Black defendants were also twice as likely as white defendants to be misclassified as having a higher risk for violent recidivism.\textsuperscript{44} Compared with violent black recidivists, violent white recidivists were 63% more likely to be misclassified as having a low risk of violent recidivism.\textsuperscript{45} The violent recidivism analysis also showed that even when controlling for prior crimes, future recidivism, age, and gender, black defendants were 77% more likely to be assigned higher risk scores than white defendants.\textsuperscript{46}

While the ProPublica report shows that risk assessment software is substantially discriminatory, the ruling in \textit{Loomis} demonstrates how difficult it can be for a court to make a legal determination that the software is so substantially discriminatory that it should not be used as a

\begin{itemize}
\item \textsuperscript{37} \textit{Id.} at 757.
\item \textsuperscript{38} \textit{Id.}
\item \textsuperscript{39} \textit{Id.} at 759.
\item \textsuperscript{40} \textit{Id.}
\item \textsuperscript{42} \textit{Id.}
\item \textsuperscript{43} Julia Angwin et al., \textit{How We Analyzed the COMPAS Recidivism Algorithm}, PROPUBLICA, (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
\item \textsuperscript{44} \textit{Id.}
\item \textsuperscript{45} \textit{Id.}
\item \textsuperscript{46} \textit{Id.}
\end{itemize}
single factor when a judge determines a criminal sentence.\footnote{State v. Loomis, 881 N.W.2d 749, 767 (Wisc. 2016).} Perhaps if the Loomis court had the ProPublica report prior to the due process hearing, the outcome would have been different. Loomis sets a tricky precedent for future cases against bad math and discriminatory algorithms.

In Loomis, the risk assessment software did not determine the defendant’s guilt, and the risk report was one factor in the court’s sentencing decision.\footnote{Id.} The court did not have to use the report at all to determine Loomis’s sentence if it did not wish to. The software was likely not strongly discredited or prohibited because of the court’s role in deciding the defendant’s sentence. Indeed, judges across the country handle increasingly overwhelming caseloads and risk assessment software can contribute to judicial efficiency.

Risk assessment software, if created properly, can also give judges objective recommendations for criminal sentencing, in which case an outright ban on these types of software might further perpetuate biased decision-making in the criminal justice system. It is possible to create unbiased risk assessment software, but to do so, like Cathy O’Neil has advocated time and again, we need to see the source code. We also need independent researchers, like ProPublica, to continue testing this software and probing these algorithms we place our blind trust in to see if they are as objective as we want them to be.

\textbf{B. Amazon Same-Day Delivery Dilemma}

In April 2016, after Amazon.com launched their same-day delivery program in twenty-seven metropolitan areas across the United States, Bloomberg News published a report showing that Amazon excluded predominantly black neighborhoods from same-day services within some six of those cities.\footnote{David Ingold & Spencer Soper, \textit{Amazon Doesn’t Consider the Race of Its Customers. Should It?}, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/} The researchers used Amazon’s publicly available data showing what zip codes were offered same-day delivery and racial demographic data from the American Community Survey to determine whether Amazon was prioritizing services to white neighborhoods over predominantly black neighborhoods.\footnote{Id.}

In Atlanta, Boston, Chicago, Dallas, New York City, and Washington, D.C., black residents were just half as likely as white residents to live in a neighborhood Amazon provided same-day delivery service to.\footnote{Id.} Amazon’s Vice President of Global Communications, Craig Berman,
responded to the Bloomberg reporters, explaining that Amazon does not use ethnic composition of neighborhoods to draw up their maps. Berman explained that Amazon’s plan is to focus its same-day service in areas where there is a high concentration of Prime members and continue to fill the gaps in the future.

Amazon offers same-day delivery service to Amazon Prime members, who pay a yearly membership fee of $99. A study from investment bank Piper Jaffray found that in 2016, around 71% of households with an average income of $112,000 and over had Amazon Prime memberships, while 43% of households with an average income between $21,000–$41,000 had memberships. Berman suggested that income inequality could likely play a role in drawing the maps, although some predominantly black neighborhoods were not given same-day delivery access despite having higher average annual household incomes than whiter neighborhoods with same-day delivery. The Amazon representative explained that too few Prime members in each area, the distance between serviced areas, the location of the closest Amazon warehouse, and the cost of the carriers create diminishing returns for certain ZIP codes. Amazon, however, does not provide the locations of the Amazon Warehouses.

Interestingly, in Boston, the Roxbury area was not offered same-day delivery, although it is surrounded by neighborhoods that have access to the service. Berman stressed that Amazon does not use race to calculate what areas are offered same-day service and that reaching the maximum number of customers is the top priority. For customers who live in neighborhoods without same-day service, Amazon’s secret formula or their intent behind it does not matter. The impact reinforces inequality in access to goods, services, and job opportunities since Amazon employs drivers and carriers within the same-day delivery communities. Moreover, these discriminatory practices could violate federal law.

52. Id.
53. Id.
54. See Ingold & Soper, supra note 49.
56. Id.
57. Id.
58. See Ingold & Soper, supra note 49.
59. Id.
60. Id.
Following the Bloomberg report, several media companies picked up the story, and politicians from Boston, New York, and Chicago called for action. United States Representative Bobby Rush, from Illinois, urged the Federal Trade Commission to investigate Amazon’s same-day delivery boundaries to determine if they violated the Civil Rights Act of 1964, for inequitable distribution services.\(^6\) In New York, State Assemblyman Jeffrey Dinowitz also called for state and federal investigations into Amazon’s same-day maps, calling the exclusion “a real slap in the face.”\(^63\) Bronx Borough President, Ruben Diaz, Jr., wrote a letter to Amazon’s CEO, Jeff Bezos, addressing the unacceptable “level of insensitivity, if not hostility” of the company’s business practice.\(^64\) In Boston, former state treasurer Steven Grossman called for residents to petition Amazon, calling the exclusion of the Roxbury neighborhood, “insensitive, unjust, and unwise.”\(^65\) Shortly following the backlash, Amazon extended same-day delivery to all zip codes in Boston, Chicago, and the Bronx borough in New York.\(^66\)

Amazon never released the method used for determining what areas would receive same-day delivery.\(^67\) Instead, Berman described multiple factors that could explain the disparate impact in select cities.\(^68\) Berman pointed to examples of predominantly minority race neighborhoods with same-day delivery in other metropolitan areas to explain that Amazon does not use race as a variable to draw up boundaries.\(^69\) Although some of the excluded neighborhoods had higher crime rates, Amazon would not say whether that was a factor involved in its decision.\(^70\) While Amazon has not given more insight into its decision-making process, Berman’s comments indicate that an algorithm, making blind assumptions based on profits and efficiency, was at play here. If humans at Amazon decided which neighborhoods to include in each metropolitan area—and perhaps that decision was reviewed by a public relations

\(^{62}\) Id.
\(^{63}\) Id.
\(^{64}\) Dan Adams et al., Why Doesn’t Amazon Offer Same-Day Delivery in Roxbury?, BOS. GLOBE (Apr. 21, 2016), https://www.bostonglobe.com/business/2016/04/21/why-doesn-amazon-offer-same-day-delivery-roxbury/09m1FLx69trWXWAK3UNgeK/story.html.
\(^{65}\) Id.
\(^{67}\) See Ingold & Soper, supra note 49.
\(^{68}\) Id.
\(^{69}\) Id.
\(^{70}\) Id.
team—the retail giant could have avoided possibly violating federal regulations.

Certainly, Amazon has no financial interest in engaging in discriminatory practices. Berman told Bloomberg, “with the math involved, we can’t make it work.” Amazon made the math work, however, and within weeks of the Bloomberg report. As of December 2017, Amazon offers Prime members same-day delivery in thirty-two cities. Amazon likely created a formula based on variables Berman discussed and other factors “the competition would kill for,” and let that algorithm dictate which ZIP codes receive same-day services. Amazon did not factor in “human” variables into their algorithm; rather, it skipped the last step human-review that the Loomis court exercised. Amazon’s “math” overlooked the importance of extending access to goods and services, as well as providing economic opportunities in these neighborhoods still struggling with economic inequality.

Like ProPublica did with the risk-assessment software used in Loomis, the analysts at Bloomberg took publicly available information straight from Amazon to detect Bloomberg’s own discriminatory algorithm. Bloomberg used its media platform to expose the disparate impact, and luckily for Amazon, it had the opportunity to right the wrong before facing legal action. Bloomberg’s report is incredibly important because it exposes how corporations may be intentionally or unintentionally practicing discrimination and how we can use data to question those practices. There is plenty of silent and invisible discrimination going on that is much more difficult to detect. Some is even illegal to detect.

C. The ACLU Takes on the CFAA in Sandvig v. Sessions

In 2016, the American Civil Liberties Union filed a suit on behalf of academic researchers, computer scientists, and journalists who wish to investigate discriminatory practices by companies on the internet. The suit challenges the constitutionality of the Computer Fraud and Abuse Act (CFAA), also known as the most hated internet law. Section

71. Id.
73. See Amazon Urged to Serve Minority Areas in Chicago, New York, supra note 61.
75. Ingold & Soper, supra note 49.
78. Id. at 1; G. Burningham, The Most Hated Law on the Internet and its Many Problems, NEWSWEEK (Apr. 16, 2016, 2:20 PM), http://www.newsweek.com/most-hated-law-internet-and-
1030(a)(2)(C) of the CFAA makes anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer” criminally liable by fine, imprisonment, or both. ²⁹ The small phrase, “exceeds authorized access,” experts argue, effectively makes any website’s terms of service law because any violation of a website’s terms of service is punishable under the CFAA. ⁸⁰

The CFAA was first drafted in 1986 and has been amended nine times as computer crimes have grown in complexity and sophistication. ⁸¹ Critics of the CFAA argue that Congress has refused with each additional amendment to narrow and define the meaning of the “authorized access” provision, create additional private rights of action, and turn misdemeanors into felonies. ⁸² Most recently, following the Sony Pictures Entertainment hack, the Obama administration promised to ensure that “insignificant conduct does not fall within the scope of the statute,” but the revision instead created harsher penalties for hacking crimes and broadened the definition of hacking. ⁸³

Some courts interpret the phrases “without authorization” and “exceeds authorized access” broadly enough to cover violations of corporate computer use restrictions or violations of a duty of loyalty. ⁸⁴ Other courts have concluded that the CFAA does not expressly forbid the misuse of confidential and proprietary computer-stored information and is limited to violations of restrictions on access to such information. ⁸⁵

its-many-problems-cfaa-448567 (The CFAA was used to prosecute Aaron Swartz after he entered a closed network closet at MIT and mass downloaded millions of academic journals; Swartz committed suicide after prosecutors rejected a plea deal).

80. Id.; Esha Bhandari & Rachel Goodman, supra note 76.
81. PROSECUTING COMPUTER CRIMES, OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS (2d ed. 2007).
84. See, e.g., United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010) (finding employee “exceed[ed] authorized access” when she used employer information, to which she had access for other purposes, to perpetrate a fraud); Int’l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (applying principles of agency, employee’s authorization to use employer’s laptop ended once he violated duty of loyalty to employer, and thus finding employee accessed computer “without authorization”); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–80, 583 (1st Cir. 2001) (interpreting “exceeds authorized access” to encompass breach of an employer confidentiality agreement where disloyal employee allegedly helped competitor obtain proprietary information).
85. See, e.g., United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (affirming dismissal of Section 1030(a)(4) charge against a defendant who resigned and then induced his former colleagues to download confidential customer information and transfer that information to him,
A broad interpretation of the CFAA’s “exceeds authorization access” provision could render activities like recording public information, providing false information, and creating multiple accounts criminal offenses. These are exactly the types of activities that researchers, journalists, and computer scientists need to do to study discrimination in big data. Christian Sandvig, one of the plaintiffs represented by the ACLU in the pending suit challenging the CFAA, explains why researchers in computing and social science need to break websites’ terms of service to investigate into potential discriminatory practices.\(^\text{86}\) They use various techniques, like writing scripts, bots, or scrapers that collect online data, to bombard closed algorithms with various inputs to study their hidden biases.\(^\text{87}\)

The ACLU represents Sandvig, three additional professors, and First Look Media Works.\(^\text{88}\) These specialists in algorithmic research want to deploy bots and use fake profiles to investigate possible racial and gender discrimination in online advertising for employment and housing.\(^\text{89}\) They also want to use automated methods of recording publicly available data from websites, also known as “scraping.”\(^\text{90}\) The websites the researchers have targeted forbid these techniques in their “terms of service,” thus the researchers cannot go forward because their actions could be prosecutable crimes under the CFAA.\(^\text{91}\)

The ACLU points out that offline audit testing, which involves pairing people of different races to pose as home- or job-seekers, has been encouraged by courts\(^\text{92}\) and Congress to uncover racial discrimination in

---


\(^{87}\) \textit{Id.}


\(^{89}\) Cyrus Farivar, \textit{To Study Possibly Racist Algorithms, Professors Have to Sue the US}, \textit{ArsTechnica} (June 29, 2016, 10:00 AM), https://arstechnica.com/tech-policy/2016/06/do-housing-jobs-sites-have-racist-algorithms-academics-sue-to-find-out/.

\(^{90}\) Esha Bhandari & Rachel Goodman, \textit{supra} note 76.


\(^{92}\) See Shaver v. Indep. Stave Co., 350 F.3d 716, 723–25 (8th Cir. 2003) (supporting “the so-called ‘tester’ cases, where minority applicants apply for jobs or housing that they have no intention of accepting for the sole purpose of determining whether the employer or landlord is unlawfully discriminating” to conclude that terminated employee’s claims were actionable).
housing and employment.\textsuperscript{93} Audit testing vindicated civil rights laws, including Title VII’s prohibition on discrimination in employment and the Fair Housing Act.\textsuperscript{94}

Specifically, the ACLU claims that the CFAA unconstitutionally prohibits the researchers’ methods of posing as online users of different races and recording information they receive, conduct the ACLU says is speech and expressive activity protected by the First Amendment.\textsuperscript{95} They further claim that the overbroad provisions within the CFAA are unconstitutionally vague under the Fifth Amendment and chill a range of speech and expressive activity by preventing private individuals from researching issues of public concern.\textsuperscript{96}

The government responded to the ACLU’s arguments in several ways. The government first argued that the plaintiffs failed to establish standing.\textsuperscript{97} It next argued that the ACLU failed to state its claims.\textsuperscript{98} It argued that the meaning of the CFAA is clear and the plaintiffs’ harm is theoretical.\textsuperscript{99}

The harm suffered from discrimination is not theoretical, however. Many of those who experience actual discrimination from an algorithmic program are not data or algorithm research specialists. It is unreasonable to expect that an average internet user has scripts, bots, and scraping tools available to audit an algorithm he or she suspects is biased. Even if a person believes an algorithm discriminated against him or her, that person likely has no avenue to request an explanation for the decision made against him or her.

III. POTENTIAL PLAINTIFFS

From where we now stand, in an era racing to apply artificial intelligence and machine learning processes in as many ways as possible, it can be difficult to imagine just how often an algorithm would be wired to discriminate against protected classes. \textit{Loomis}, the Amazon same-day dilemma, and \textit{Sandvig} provide examples of suspicious algorithms that needed auditing.

\textbf{A. Artificial Intelligence & Image Recognition Software}

Machine learning and artificial intelligence create more significant room for error because of their unique mechanism of “training” a data

\begin{thebibliography}{99}
\bibitem{94} Shaver, 350 F.3d at 723–25.
\bibitem{96} Id.
\bibitem{97} Memorandum of Points and Authorities in Support of Defendant’s Motion to Dismiss at 2–3, 8–9, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).
\bibitem{98} Id. at 2–3.
\bibitem{99} Id.
\end{thebibliography}
set. Take, for example, how a computer science professor discovered that image-recognition software “learned” to associate images of shopping, cooking, and cleaning with women; and pictures of coaching, shooting, and sports with men. This image-recognition software used machine learning, taking a seemingly unbiased dataset, “learned” about those datasets, and amplified that training on future datasets. The image-recognition software took collections of pictures of both men and women and identified various other items in the background of those pictures. The software found that within the dataset, women were in more pictures with items found in the kitchen, and men were in more pictures with sporting equipment. After the image-recognition software was “trained” on these datasets, it amplified gender bias in future data sets, misidentifying a picture of a man cooking on a stovetop as a woman.

In 2015, Google’s image recognition software mistakenly labeled photos of black people as “gorillas.” Google swiftly updated the malfunction. After Apple introduced iOS 10 in 2016, a twitter user found that the iPhone Photos application was capable of recognizing photos containing “brasieres,” a keyword included in the object and scene detection software. A list of the searchable keywords in Apple’s scene and object detecting software update contains words including, “bra,” “brasiere,” “corset,” and “girdle;” but does not include “underwear,” “boxers,” or “briefs.”

If the researchers who created the initial dataset selected more photographs of women in undergarments than men in theirs, the object-detecting software will prioritize, categorize, and “learn” more about the objects that appear most often in the initial dataset.

101. Id.
102. Id.
103. Id.
108. See Simonite, supra note 100.
studies showing that most job positions in the tech industry are filled with men might partially explain how more photos of “brassieres” slips into an initial dataset. These examples of image-recognition software gone awry show us how easily bias can proliferate from a program’s initial dataset and amplify that bias. Although patently offensive, many still underestimate the legal implications of image-recognition software misidentification or its malicious use. As artificial intelligence technology advances at such a high pace, so does the severity of its misapplication. In a recent study, researchers found that facial recognition software could detect a human’s sexual orientation significantly better than a human could. A misapplication of this “Gaydar” technology could allow advertisers to target specific products to a person based on his or her sexual orientation. But in a country where homosexuality is a punishable crime, it could expose a substantial threat to the personal privacy and safety of gay men and women.

B. Advertising Left on Auto-Pilot

Misidentifications and misapplications of face-recognition technologies illustrate how blind faith in algorithms threatens individual privacy. Although big data companies largely insulated themselves from discrimination claims via targeted advertisements, ProPublica found that Facebook gives advertisers the ability to exclude groups of individuals based on their “ethnic affinities.” While Facebook does not ask its members about their specific race, it mathematically assigns users an “ethnic affinity” based on pages, posts, and engagement with other users’ content.

Journalists at ProPublica purchased an advertisement for Facebook’s housing categories and, in the Detailed Targeting feature provided,

114. Id.
excluded anyone with an “ethnic affinity” for African-American, Asian-American, or Hispanic people. The advertisement was approved within fifteen minutes of placing the order. This practice clearly violates the Fair Housing Act of 1968. ProPublica went on to find 50,000 unique metrics Facebook measures its users by and uses for targeted advertising. Although Facebook prohibits advertisers from using the targeting options for discrimination, harassment, disparagement, or predatory purposes, that policy did not prevent ProPublica’s housing advertisement or ads that target people with interests such as “History of ‘why jews ruin the world.’” The social media giant reportedly made $26.89 billion in advertising revenue in 2016.

While Facebook has continued to enhance its efforts to regulate content, its current policy—manually removing advertisements that violate its anti-discrimination policies—is borderline negligent. Facebook’s advertising revenues continue to increase, just as the number of its advertising-related scandals. While media organizations like ProPublica and Bloomberg have successfully investigated discriminatory-promoting algorithms, Facebook has taken more measures to obfuscate its advertising stats. For a corporation capitalizing on its incomprehensible level of user engagement, concealing the secret formulas for targeted advertising seems like a C.Y.A. effort at best and fraudulent at worst. Facebook, like other big data companies, does not want the liability of researchers finding bias and discrimination hidden in its algorithms because its monetized model depends on it. Moreover, if Facebook allowed researchers to examine its math for insidious bias, researchers might find out that Facebook’s...

115. Id.
116. 42 U.S.C. § 3604(c) (2012) (“it shall be unlawful . . . to make, print, or publish, or cause to be made, printed, or published any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin . . . “).
117. Id.
advertisements are not as valuable as businesses believe they are in the first place. Either way, Facebook has no financial incentive to be transparent—unless the public holds it accountable.

IV. CHALLENGING ALGORITHMS

Big data companies need constant public pressure to keep their practices transparent. Besides the third-party review of publicly available information provided by these corporations, there are substantial legal hurdles for researchers to overcome when they suspect algorithmic discrimination.

Limiting the scope of the CFAA so that academic researchers can violate websites “terms of service” to study potential discriminatory practices would substantially advance the cause. Following the filing of the complaint in Sandvig, ACLU Staff Attorney, Rachel Goodman, published an article outlining some suggestions for data journalists.123 She explains that one way to circumvent the CFAA entirely would be to directly ask the company for permission to audit its algorithmic processes.124 That would give the researcher “authorized access,” but it might also legally implicate a researcher who chooses to go forward with the research without permission.125 Goodman also recommends carefully choosing which technique to use before investigating so that a researcher can avoid damaging a target company’s servers, computers, or interfering with its regular business operations.126 An option of last resort for researchers who have been accused of violating the CFAA should be to draft a defense based on civil rights enforcement.127

Goodman illustrates how Congress and courts have encouraged and recognized audit testing in the offline fair housing and employment contexts, as they should in the online context.128 While the ACLU attempts to tackle head-on the “exceeding authorized access” provision in the CFAA in the judicial system, there is support across the web for legislatively amending the Act to clearly define “authorization” and the penalties for violation.129

In the meantime, some algorithmic-justice warriors are challenging blind faith in algorithmic decision-making in their local communities.

124. Id.
125. Id.
126. Id.
127. Id.
128. See id.
This year, James Vacca, a Democratic City Councilman from the Bronx in New York City, introduced a bill that would require the city to make public any computer instructions or algorithms that the government uses for any type of automated decision-making.\footnote{130} Increasingly, city governments are applying algorithms to decide which neighborhoods receive the most policing, which schools students are zoned for, and where to conduct health and safety inspections.\footnote{131} Vacca’s bill would require transparency with regards to the code used in any of the local government’s decision-making algorithms as well as audits for any algorithm leased by the city from private companies.\footnote{132}

Abroad, the European Union has been more aggressive toward anonymous algorithms.\footnote{133} The General Data Protection Regulation is scheduled to take effect in 2018 and has been highly publicized for its establishment of a “right to be forgotten,” but also includes a “right to explanation.”\footnote{134} The law will restrict algorithms that make decisions based on user predictors which make decisions about them.\footnote{135} The “right to explanation” gives users an avenue to request an explanation of an algorithmic decision that was made about them.\footnote{136} Critics of the new law say that this will make it more difficult for tech companies to develop more complicated algorithmic systems, thereby hindering innovation in the field.\footnote{137} Oxford researchers Bryce Goodman and Seth Flaxman argue, however, that the implementation of the law gives computer scientists the opportunity to develop algorithms that avoid discrimination and enable explanation.\footnote{138}

\begin{footnotes}
\item[135] Id.
\item[136] Id.
\item[137] Id.
\item[138] Id.
\end{footnotes}
CONCLUSION

For many millennials, America has never felt as divided as it feels at the end of 2017. Academics have updated curricula in social science, history, and literature to reflect inclusivity and diversity; and to eliminate bias, stereotypes, and discrimination. Academia has mostly left mathematics, science, and technology out of discussions around race, color, nationality, sex, sexual orientation, and economic class. That needs to change now more than ever.

As big data companies continue to measure intimate human traits in every imaginable way, those companies desperately need to be engaged in meaningful ethical discussions on implicit and explicit bias. Debates will rage on over whether we have done enough to combat bias, hate, and bigotry. But it is time to hold the creators of discriminatory algorithms accountable. It is time to expose corporations’ advancement of systemic prejudice and tackle it head-on. Whether we amend the CFAA, continue placing public pressure on discriminatory business practices, or create new laws requiring transparency of these hidden algorithms, we need to end the era of placing blind trust in big data and take control over the machines that are taking control over us.
CASE COMMENT

EXTRATERRITORIAL APPLICATION OF DATA PRIVACY LAW: HOW THE STORED COMMUNICATION ACT LAGS BEHIND MODERN TECHNOLOGY

Andrew Bayudan*

I. OVERVIEW

The Stored Communications Act (SCA),1 which allows the government to compel the production of electronic customer information from Internet Service Providers (ISPs), was found to be limited in scope by the Second Circuit in Microsoft Corp. v. United States.2 The Second Circuit ruled that the SCA did not permit the government to force ISPs to hand over data that is located outside the United States.3

In 2013, a warrant served under the SCA, was authorized requiring Microsoft to produce information and emails related to a federal criminal investigation.4 Many of the emails demanded by the warrant were located on a data server in Ireland.5 Since these emails were outside the United States, Microsoft argued that the warrant under the SCA had no jurisdiction in Ireland and moved for the warrant to be quashed.6 The magistrate judge denied the motion.7 The denial was also affirmed by the Southern District of New York, reasoning that the SCA compelled those served with warrants under the SCA to produce information regardless of the information’s location.8 Microsoft appealed the district court’s decision,9 held that the district court’s denial of microsoft’s motion to quash the warrant was improper and the case should be reversed and remanded to the district court.10

* Andrew Bayudan, J.D. Candidate, May 2019, University of Florida Levin College of Law. I would like to thank my family for their love and support.

2. Microsoft v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016).
3. Id.
5. Microsoft, 829 F.3d at 200.
6. Id. at 200–01.
7. Id. at 201.
8. Warrant to Search, 15 F. Supp. 3d at 477.
9. Microsoft, 829 F.3d at 200.
10. Id. at 201.
II. BACKGROUND

A. Microsoft’s Email Services

Microsoft is an ISP headquartered and incorporated in the United States. Microsoft provides free online email services to the public. When creating an email account, users are asked to indicate their location of residence. The information associated with a user’s account, along with the emails sent and received through the account, is stored on physical servers that are housed in large datacenters. The datacenters are generally located near the location the user initially indicated when creating the email account. This email service is offered to customers in over 100 countries and Microsoft maintains datacenters in over forty countries.

Though Microsoft’s datacenters are located worldwide, the company is able to manage and collect information on servers in other countries through its database management computer program from the United States. This computer program can be accessed in offices in the United States. Additionally, this computer program allows Microsoft to retrieve data located on servers in other countries and store it on servers in the United States. Therefore, Microsoft employees in the United States do not need to travel outside the United States to collect information from servers located in other countries.

B. The Stored Communications Act

The U.S. Government served a warrant on Microsoft to produce certain electronic information under the authority of the SCA. In 1986, the SCA was passed to protect American privacy interests in response to the rapidly evolving and advancing technologies that developed alongside the personal computer. The SCA prohibits unauthorized parties to access or modify electronic communications maintained by ISPs. Yet, the SCA also contains a provision that requires ISPs to

11. Id. at 202.
12. Id.
13. Id.
14. Id.
15. Id.
16. Id.
17. See id. at 203.
18. Id.
19. Id.
20. Id. at 205.
21. Id.
22. Id. at 207; see 18 U.S.C. § 2702 (2012).
provide data that the government so requests with a warrant, pursuant to the Federal Rules of Criminal Procedure. The SCA did not, however, contain any provisions that address whether the issued warrants would be applied to electronic communications outside the United States.

C. The SCA’s Extraterritorial Scope

A two-part test adopted from Morrison v. Nat’l Austl. Bank Ltd. to determine whether the SCA can apply to extraterritorial electronic communications is used to interpret the SCA. The first part of the test looks at whether the statute’s language suggests extraterritorial applications. When interpreting a statute, there is a default presumption that Congress enacted the statute with the intent to apply the statute only within the United States. This part of the test requires that the statutory language has a clear indication that the statute would apply extraterritorially.

For the second part of the test, it has to be determined whether the application of the statute in the disputed case is an unlawful and extraterritorial application. In this part of the test, the facts surrounding the case and the statute’s focus are examined.

D. The District Court’s Reasoning

The district court, finding that the SCA warrant could be enforced extraterritorially, focused on the ambiguity of the SCA’s use of the word “warrant”. The district court stated that a warrant, in the context of the SCA, actually is a hybrid of a warrant and a subpoena. The SCA warrant is like a traditional search warrant because the SCA warrant must be obtained by following the Federal Rules of Criminal Procedure. The SCA warrant is like a subpoena because the receiver of the SCA warrant

24. Microsoft, 829 F.3d at 208.
27. Id.
28. Id.; see also Morrison, 561 U.S. at 247.
29. Microsoft, 829 F.3d at 210.
30. Id.
32. Id. at 471.
33. Id. at 470.
must provide the requested information no matter the information’s location.34

The district court also considered the practical effects of not compelling Microsoft to produce the email data from extraterritorial servers.35 By not compelling Microsoft to do so, criminals could simply avoid SCA warrants by moving their servers to other counties.36 This would also result in the government having to turn to Mutual Legal Assistance Treaties (MLATs) to obtain information stored extraterritorially.37 MLATs are international agreements where one country can request assistance from another country with criminal investigations that have effects in other countries.38 Since MLATs rely on the cooperation of another country’s government, MLATs often operate very slowly.39 Additionally, the United States does not have MLATs with many countries, making it easier for criminals to avoid SCA warrants.40

III. THE INSTANT CASE

In the instant case, the Second Circuit applied the two-part Morrison Test to determine whether or not the warrant under the SCA could be applied to the email located on servers in Ireland.41 Reversing the district court’s decision, the Second Circuit decided that the SCA warrant could not compel Microsoft to produce data located on Ireland’s servers.42

For the first part of the Morrison test, the court found that Congress did not expressly indicate their intent for the SCA to apply extraterritorially.43 There is no textual or documentary support to suggest that the SCA applies extraterritorially and reading the SCA to have an extraterritorial scope is arbitrarily expanding the SCA’s reach.44

The court further explained that the district court’s interpretation of the word “warrant” was incorrect.45 The court found that the district court inappropriately interpreted “warrant” as having a hybrid meaning.46

34. Id. at 471–72.
35. Id. at 474–75.
36. Id.
37. Id. at 476.
38. Id.
39. Id.
40. Id.
41. Microsoft Corp. v. United States, 829 F.3d 179, 210 (2d Cir. 2016).
42. Id.
43. Id. at 211.
44. Id.
45. Id. at 212.
46. Id. at 210.
Instead, the court held that “warrant” under the SCA had a meaning only related to the privacy protections granted by the Fourth Amendment.47

Turning to the second part of the Morrison test, the court determined that using an SCA warrant to compel Microsoft to produce electronic information located on a server in Ireland was an extraterritorial application of the SCA.48 The SCA was primarily enacted to protect and focus on citizens’ privacy, as evidenced by the SCA being part of the larger Electronic Communications Privacy Act.49 Further, the SCA’s warrant to Microsoft was being used to assist a criminal investigation, rather than protecting a citizen’s privacy interest.50 The SCA warrant issued to Microsoft targeted information on data servers located in Ireland.51 Because the focus of the SCA warrant was a privacy interest that existed in Ireland, this application of the SCA was extraterritorial and outside the SCA’s scope.52

IV. ANALYSIS

This case was decided incorrectly because the court failed to consider the technological advancements that have occurred since the initial creation of the SCA. The SCA was passed in 1986, where the state of technology was vastly different and inferior to the state of technology today. Since 1986, both the amount of storable data and the easiness of storing data have greatly increased, while the cost of storing data has decreased. Additionally, developments in the internet have made it very easy to transport and store data across large distances at extremely fast speeds. When the SCA was initially passed, these advancements were likely never considered or realized. Many of the technological obstacles that existed in the 1980s that posed practical problems in extraterritorially enforcing the SCA warrant no longer exist today.

Microsoft, like many other large corporations that maintain large amounts of electronic data and have numerous customers around the world, has data located in many other countries. Microsoft can easily move data on one country’s server to another without much burden or cost to the company. To limit the enforcement of an SCA warrant to only data located on servers within the United States would obstruct government and criminal investigations. This limitation makes little sense in a world where large amounts of data is constantly moving across

47. Id.
48. Id. at 213.
49. Id. at 217.
50. Id.
51. Id. at 216.
52. Id. at 220.
borders at high speeds with little cost. The court, rather than looking at where the data servers are located, should have given more weight to where the ISP was located and the extent of the ISPs business in the involved countries when determining if the SCA warrant could be enforced.

This case also exemplifies how the SCA’s language and goals have been outdated and outpaced by technology. The SCA lacks many of the considerations and concerns that have developed since its enactment. The court, rather than choosing to acknowledge these advancements, chose to adopt a limited and archaic view of the SCA that prevents the court from fully addressing the issues in this case.

V. CONCLUSION

The decision in Microsoft Corp. v. United States challenged the scope of the SCA. The Second Circuit, not taking into account the numerous technological advancements since the SCA was passed, incorrectly limited the enforcement of SCA warrants to only data that exists domestically. This decision could have many undesirable consequences, including criminals avoiding government SCA warrants. These issues will continue to exist and pose problems for courts as technology rapidly evolves.