2022

Forgiving Without Forgetting? Privacy in an Age of Digital Permanence

Rock Park
Macalester College, rockpark225@gmail.com

Forgiving Without Forgetting? Privacy in an Age of Digital Permanence

Rock Park
Honors Thesis – Macalester College Department of Political Science
Advised by Patrick Schmidt
Submitted April 27, 2022

"American culture is rich in the belief that an individual can pull up stakes and make a fresh start, but a universally identified man might become a prisoner of his recorded past." -- U.S. Department of Health, Welfare, and Education (HEW), "Report on Records, Computers, and the Rights of Citizens" (1973).

Abstract

The 21st Century has been marked by increasing digital globalization, and an extensive, complete record of most individual's public and private lives. This posed enough of a risk to privacy that in 2014, the European Union began to outline and articulate the digital privacy rights of European citizens in a set of policies known as "right to be forgotten" laws. As of 2018, these right to be forgotten protections had been codified into the General Data Privacy Regulation for the EU (GDPR). This paper explores the construction of privacy and subsequent adoption of the right to be forgotten specifically in France, relative to the divergent evolution of privacy—and lack of digital privacy protections—in the United States. Namely, this paper compares the right to be forgotten as a potential tool of rehabilitation in conjunction with criminal expungement practices and considers the connections between a punitive criminal justice system and digital remembering.

Table of Contents

Acknowledgements

I would like to thank Patrick Schmidt for his enthusiasm, constructive feedback, and for holding me accountable throughout such a long process. Thank you for sharing your legal expertise with me, for guiding me in the right direction, and for encouraging me to not let 'perfection be the enemy of good.' Thank you, Lesley Lavery, for your optimism and encouragement, and for pushing us along and getting us through our early morning meetings. I'd also like to thank Paul Dosh, for advising me throughout my time at Mac, and for pushing me to do an honors thesis.

To my honors cohort—Cande, Sophia, and Lucien— thank you for your constant support and for holding me accountable, for talking through the challenges of this project, and for late night draft-editing.

And to my family, thank you to my parents for sending me love from afar, and for staying through mid-dinner Facetime calls. Thanks to Sophie and Mikey for their support, sympathy, and solidarity in being overworked and underpaid.

I would also like to thank my roommates, Margot and Niko, for putting up with dirty dishes and an absentee roommate.

Section I: The Arrival of a New Privacy Right

In a 2010 case in the Spanish courts, a Spanish citizen filed complaints against Google and Google Spain to remove links to a decades-old news article which referenced a property he owned which had been foreclosed due to nonpayment. The Spanish Data Protection Agency (AEPD) ruled in favor of the plaintiff, and that Google Spain must delete links to the article since the information was outdated. Google appealed this decision, and in 2014, the judicial branch of the European Union, the European Court of Justice (CJEU), ruled again in favor of the plaintiff and his "right to be forgotten," stating that search engines must respond and remove information upon request, about any information deemed "inadequate, irrelevant or no longer relevant, or excessive" (Dowdell, 2016, p. 319). These key rulings in these cases eventually resulted in a new EU-wide proposal being drafted, known as the General Data Protection Regulation (GDPR). The GDPR became codified into law in 2018, replacing the 1995 Data Protection Directive, and granted all citizens of EU member states a more narrowed "right to erasure," which allows citizens the right to petition data controllers and processors for removal of information (Art. 17(2), GDPR). While the right to be forgotten reflects advances in privacy in digital spheres to better protect individuals residing in the EU, competing interests between internet service providers and private citizens required drafting laws that attempt to find a balance between the public's right to know and privacy concerns of individuals.

The right to be forgotten is a personal data statute which allows individuals to petition search engines for removal of certain truthful information about themselves

online. Defined as both a "right to delete" true-but-outdated information about oneself, as well as a "right to control information about oneself," the right to be forgotten applies existing privacy doctrine to emerging digital contexts. The right to be forgotten emerged in the European Union over the past three decades from a desire to provide data protection to citizens, and out of a centuries-long commitment to the principles of privacy as identity formation. In the Google v. Spain case, the plaintiff argued that the continued publication of this true-yet-outdated information was violating their privacy via the 1995 Data Protection Directive (95/46/EC), which asserts that data processing must "respect their fundamental rights and freedoms, notably the right to privacy" (Directive 95/46/EC, Article 2). Now called "the right to be forgotten," "the right to delete," or the "right to erasure," the basic tenets of the right to be forgotten have incorporated a more nuanced understanding around memory in their interchangeability. As Antoon deBaets argues, the right to be forgotten implies forcing another to forget about an individual's past actions, as "an act of coercion in the realm of holding and expressing opinions" (de Baets 2016, 8). Rather, the 'right to erasure' or its synonym, 'the right to delete,' both highlight the power of the individual to remove information about themselves without coercive language or a power willing another to forget. For the purposes of this paper, "the right to be forgotten" will be used as the policy name in general, with occasional inclusions of 'the right to delete or erase' for specific mentions of removal of information.

Thus, the right to be forgotten emerged as a mechanism used to assess, process, and potentially de-list the overwhelming amount of information available to everyone through a few keystrokes of a Google search. Whether it is related to the latest celebrity

drama or a decades-old story of criminal wrongdoing, the internet preserves a comprehensive digital memory that is more accessible and more complete than what any individual is capable of remembering (Mayer-Schönberger, 2009). However, the laws around punishment and wrongdoing have not kept pace with this onslaught of information; the societal and legal values of transparency over privacy have ensured that rehabilitation after wrongdoing has not been a priority considered by current laws or statutes.

Although the right to be forgotten has many proponents beyond the European Union, other countries—such as Canada, Australia, and the United States—oppose the measure. Considered by many U.S. scholars to be a blunt tool to parse the delicate balance between the right to privacy of an individual versus the right to know of the masses, the right to be forgotten has yet to take root in U.S. federal policy. Simultaneously, state courts and legislative bodies have been seeking other solutions to the growing concerns around people with records of incarceration facing barriers to re-entering mainstream society. A criminal record in the age of instant recall becomes a huge financial and social barrier to normal life.

While many U.S. states are currently pushing for laws on digital criminal expungement to alleviate the burden on the American populace from histories of incarceration, this aim may be "too-little-too-late" to allow individuals to move past transgression. Likewise, there are understandably many instances where the public would want to know people's criminal records, such as whether someone has committed acts of sexual violence, or the tangible harms caused to victims of an individual's wrongdoing.

The inclination towards forgiving past offenders tends to be at-odds with forgetting, even though rehabilitation stands to encourage both recognition and forgiveness of the tough task of reconciling acts of harm in community. Given the role of digital memory in preserving histories of wrongdoing, what mechanisms for forgiveness, intentional forgetfulness, or remembrance have different countries developed for dealing with the past? How do these new policies and statutes in other countries reflect a potential pathway for some U.S. right to privacy, particularly concerning criminal records? In this thesis, I attempt to reconcile scholarship around stigma and criminal convictions, and the importance of a right to privacy despite an individual's past, within the context of the existing legal and cultural context of the U.S.

The first section of this thesis provides background on the right to be forgotten and the emergence of new manners of controlling one's image online that have emerged from the European Union, with detail towards looking at the applicability of these forgetful policies to people with records of wrongdoing. In section II, I will explore the relevant scholarship on privacy and the pressing needs for digital reforms to extend to criminal justice spaces around privacy and preserving community. Through combining scholarship on collateral consequences and the role of the carceral state, I situate the right to be forgotten as a powerful tool of forgiveness, in allowing individuals some manner of separation from their past actions, giving this mechanism for intentional forgetting particular significance for people with criminal records. I also discuss my theoretical framework and case selection in choosing France as a comparative analysis to the United States. Section III develops the case of France, which has become the most prolific

enforcer of the right to be forgotten in the EU and extends rights to privacy to all manners of citizens, regardless of their criminal status. Section IV discusses the barriers to developing a right to privacy in the United States, and how this has formed an insurmountable barrier thus far to enacting comprehensive digital privacy and erasure rights for U.S. consumers. Section V takes existing reforms in the United States and attempts to situate lessons from the French case within the U.S. context.

Section II: Literature Review

In the United States, France, and the rest of the world, social developments have coincided with these questions of digital privacy, such as reconciling an individual's social and legal rights of privacy with broader access to information. However, while laws around digital privacy are being considered, co-evolving changes have been happening in the criminal justice sphere. Given the adverse consequences of having a criminal record, many countries (and some U.S. states) are grappling with how records of incarceration fit into current social and digital frameworks. Many third-party websites have emerged to re-publish and continue to circulate private court information about carceral histories of individuals, even in cases where the individuals have been able to expunge their record in courts, and where individuals may not have even been convicted of a crime. While the information has always been public in the United States, the internet has substantially lowered the cost of accessing the information of others. Thus, the internet's generative capacity allows for the publishing of truthful information;

however, it also releases information that would have never been circulated through analog pathways.

The right to be forgotten is just one possible pathway for confronting the onslaught of digital information. In this section, I will discuss literature that looks at how changes in the availability of information have affected the experiences of individuals who pass through the criminal justice system, and then review the existing literature on the construction of the right to be forgotten within a larger context of digital privacy and identity. Combining this scholarship informs my theoretical framework around policy developments, and the social concerns around wrongdoing and rehabilitation that emerge in contemporary discourse of criminal justice.

Collateral Consequences and the Need for Reform

The application of digital privacy to cases of criminal wrongdoing exposes the differing pathways through which a criminal record can affect someone's life, even decades after one's transgression. Comparative criminal justice scholars have established connections between punishment and an international trend towards harsher sentencing, more punitive systems, and more consequences for wrongdoers, with the United States leading the trend. Indeed, many scholars articulate how America's criminal justice system is one of the most punitive in the world, with racially stereotyped trends resulting in a disproportionate incarceration for BIPOC populations (Tonry 1994, 2010a; Alexander 2010; Walker 2010; Hinton 2016). The U.S. has also experienced a record increase in the number of people incarcerated, and now has the world's largest incarcerated population and rate of incarceration, with 2.2 million incarcerated people in

2010 and a rate of incarceration of 738 per 100,000 people (Steiker 2011, Hartney 2006). The basis for this increase in incarceration, these scholars argue, bears no correlation to actual increases in crime rates; rather it is due to more punitive sentencing policies. Tonry and Alexander trace this heightened record of racialized incarceration to the War on Drugs in the 1980s and 1990s, a political attempt to employ zero-tolerance crime deterrents such as increased street-level policing in predominantly minority-populated urban environments, resulting in an exponential increase in incarceration continuing to the present. Tonry (1994) asserts that the politicized push for crime control, often advanced by conservatives within both the Republican and Democratic parties, has resulted in policies that uphold the War on Drugs campaigns of the Reagan and Bush presidencies and champions highly punitive measures such as three-strikes policies and mandatory minimum sentencing (Tonry 1994, 488). Broadening the discussion of incarceration, Alexander (2010) maps out the problems of the prison-industrial complex more broadly, including a lengthy discussion on the connections between criminal records and prolonged exclusion from society and difficulty of re-integration post-punishment. Given the United States' higher rates of policing and incarceration relative to other countries, the issues faced by individuals who have some type of a criminal record are relevant for looking at the long-reaching consequences of incarceration.

Facing what are often called collateral consequences, many former inmates (as well as people who are booked temporarily and released) face barriers to re-entering society; these can be the systematic denial of rights through legal means, such as voting in elections, or social norms of exclusion, such as difficulty with employment or finding a

place to live. Downes (2001) adds another dimension to this argument by suggesting that collateral consequences of incarceration are neither accidental nor vestigial. These increasingly harsh post-imprisonment sanctions are by design, Downes argues, and "the removal of criminals from American society by penal means" creates the perception that a utopian society can now be achieved (Downes 2001, 66). Chin (2012) builds on this argument by discussing how the framework of civil death, suggesting that incarceration and time served can actually be one of the milder consequences of the U.S. criminal justice system, and that "the most severe and long-lasting punishment is not incarceration, but the collateral consequences of losing civil rights, public benefits, etc." (Chin 2012, p. 1791). Chin (2012) continues this discussion of collateral consequences to explain how contemporary punishments in the U.S. have historically been situated in common law courts to legally alienate wrongdoers from the rest of society and stigmatize their actions as socially unacceptable. Whether this means keeping people on parole or probation for years after imprisonment, losses of legal status or civil rights, or preventing former convicts from voting, lifelong consequences can debilitate one's life, even without serving jail time. This network of far-reaching barriers to reintegration has the potential to affect everyone who has either been convicted or arrested, which works out to between 70 and 100 million Americans having some type of criminal record that prevents or slows rehabilitation (Vallas 2014, 1). Other scholars argue that this mechanism of social control and stigma is intentional; Kantorowicz (2014) and Aebi (2015) both argue that the increased variety of incarceration options aims to increase rather than decrease the number of people under state surveillance. In explorations of community sanctioning in

the U.S. (Kantorowicz, 2014) and in Europe (Aebi, 2015), both scholars argue that allowing for probation, parole, electronic monitoring services, and community service simply "transfers criminals from custody to community"; that is, it puts the enforcement of good behavior on society rather than prisons, but it effectively serves as a mechanism for social control, causing a net-widening effect of people under the watch of government and within existing networks of surveillance (Kantorowicz 2014, 4; Aebi 2015, 589). Thus, wide-reaching reforms in criminal justice often serve to broaden the scope of surveillance in the name of crime prevention.

The net-widening effect in criminal sanctioning raises many questions about the nature of punishment and the internet's role in transferring the responsibility of generating stigma from the state to community members. Many scholars of comparative criminal justice and the sociology of punishment demonstrate how the collateral consequences of incarceration or conviction have far-reaching implications in the digital age. Lageson (2016) explores both the psychological and economic impacts of having a low-level criminal record. People with records avoid the increased visibility and potential for discovery of their past that comes with higher-paying jobs and upward mobility and experience a "systemic avoidance" of social and institutional support for people with records (Lageson 2016; 136). In interviews with expungement-seekers, Lageson characterizes the fear of discovery felt by many people who are unlikely to apply for jobs that require background checks, social media reviews, or online search results, and she argues that privately run websites and mugshot databases undermine the existing legal system of courts sealing and expunging records. Haber (2018) further contextualizes the

challenges of digital criminal expungement; she first outlines the rehabilitative goals of expungement, which aims to reduce recidivism and discrimination against formerly incarcerated people, and to reward people who work to reintegrate themselves back into society. However, given easy online access to criminal histories, "digital data practices make expungement statutes almost inapplicable, and even potentially facilitate a market for expunged criminal histories" (Haber 2018, 351). Calvert and Bruno (2020) continue this discussion around expungement laws; although the lived realities of people who seem unable to forget their past are dire, pathways for expunging information are limited in efficacy, particularly in the United States, against the First Amendment freedom of expression. The tension that arises between the First Amendment's implicit 'right to know' of the public, and the personal control of information privacy is central to the issue of where the line between public and private lies, especially concerning the potential long-term disadvantage of having a criminal record or an arrest record. Calvert and Bruno (2020) argue that, even in cases where the freedom of expression of the media reveals the truth, these digital records may only tell a partial yet permanent account of a given set of events, where "stories regarding the arrest and charging of an individual—regardless of the outcome of the case…languish and linger in perpetuity in cyberspace and be easily discovered through a few keystrokes on a Google search" (2020, 126). Even with existing pathways for criminal record expungement, the digital recording and republication of offenses has become ubiquitous; technology and widespread access to information has changed the consequences of any interactions with the criminal justice system. Digital publication of crimes, alleged crimes, or other instances of wrongdoing not only place an

emotional and anxiety-provoking strain on the individuals named, but also place a burden on society through the complex balancing act between an individual's right to personal privacy and other citizens' right to know. If third-party databases exist for mugshots, criminal proceedings, and other conviction information, it does not matter whether information is expunged from the court records, as other citizens can easily access former arrest records, convictions, or other potentially damning information (Calvert 2010). Thus, issues of digital permanence challenge existing rules and regulations, such that the U.S. system does not provide easy answers for people wishing to move beyond their past transgressions.

Laws of Reputation and Personality Rights

The long-term consequences of incarceration and inability to return to society underscore the pressing need for policy reform. Whether on social media, captured in news articles, or regrettably posted by an individual, all kinds of digital information populate archives, and can have the same damaging reputational effects that records of incarceration have.

Different countries have proposed many different mechanisms to ensure protection of their citizens' dignity and virtual privacy. Whereas some countries impose mandatory privacy policies to educate consumers about their digital footprints, others enact digital protection regulation. In the United States, the approach has mainly centered around this privacy policy approach; however, the norm has tended towards non-regulation and leaving individuals to make their own decisions about internet use. While the United States has been slow to deal with the onslaught of challenges posed by the

internet, other countries have made considerable strides in evaluating and acknowledging information about individuals online.

One of the key ways different countries have proposed to deal with these long-term consequences has been to look at the publication and recirculation of information as a privacy and reputational matter. Whitman (2004) contends that historically rooted conceptions of privacy in continental Europe and the United States inform modern questions of privacy today, and the framing of the right to privacy as either a "dignity" or "liberty" has broad implications for the type of protections a right to privacy can grant. Whitman (2004) argues that while "perceptions of privacy" differ between Western European countries and the United States, the commitment to privacy as a personal value (and a value deserving of legal support), has robust theoretical support in both jurisdictions (p. 1159). For example, Whitman uses the case of France to articulate how honor used to be something reserved for people of status or wealth, yet the French Revolution allowed for all citizens to benefit from incorporating privacy into the "law of respect and etiquette" (2004, 1167). Constructing privacy as an intrinsic personality and identity-building component has created a "right to a public image of our own making, as the right to control our public face" (Whitman 2004, 1168). In contrast, Whitman proposes, the U.S. framing of privacy as a "liberty" reflects a history of distrust of the State and worries about infringement upon one's home and private life by government actors. While the continental construction of privacy focuses on the potential for "personal or moral injury" from media, the U.S. understanding of privacy focuses on preventing "invasions from government…invasion of his indefeasible right of personal

security and private property" (Whitman, 2004, 1212). Through comparing cultural and historical constructions of privacy, the differing laws and policies around digital privacy reflect the existing cultural and legal norms of a country.

The Right to Be Forgotten: Adapting for the Digital World

Amid these opposing constructions of privacy before the digital age, different countries have enacted (or refrained from implementing) drastically different conceptions of digital privacy and the role of the consumer and citizen. These contrasts can perhaps best be seen between the European Union member states and the United States. Whereas the EU has enacted many of the foundational texts and policies for right to be forgotten laws, the United States has been slow to confront the many problems faced by increasing access to information. Historically, the American approach to information has favored freedom of the press and freedom of speech, and deregulation of industry to allow the free market to run its course, all of which have set the stage for a culture that values transparency and the public's right to know more than the ideal of privacy.

Digital privacy laws in the EU allow an individual to petition for removal of truthful information if a certain amount of time has lapsed, or other qualifications around time and active rehabilitation are undertaken. In contrast, the United States has a centuries-long protection of freedom of the press, in order to ensure the media's ability to serve as a watchdog on government, circulate truthful information, and provide transparency to U.S. citizens. This has resulted in a "transatlantic clash" between the E.U. and the U.S. in terms of privacy rights (Rustad & Kulevska 2014, 376). Leta-Jones (2016) articulates in *Ctrl + Z* how existing legal cultures have foreshadowed these

divergent paths through the development of the right to be forgotten laws in Europe, while the prevailing legal conditions of the United States have largely been unfavorable to a right to be forgotten. Tech conglomerates based in the United States are forced to cooperate with European data protection agencies to enforce the right to be forgotten, while legislation for these tech companies in the United States lags behind these EU standards, and often takes a decidedly pro-business stance against consumer privacy protections.

Where does this leave the United States on digital privacy rights? The U.S. commitment to the First Amendment freedom of press forms a fundamental obstacle to removing old information, regardless of whether it is relevant given a person's transformation or growth. The United States has strong protections for freedom of the press, and this only implies a right to privacy, defined by Werro (2009) as "a series of attempts by the various states to carve out for their citizens a sphere of individual privacy inviolable from the mass media" (p. 292). In contrast, the logic for granting the right to be forgotten in the European Union rests on the need to equally balance the public's right to know with an individual's right to personal privacy—a right recognized under the European Convention on Human Rights (Article 8, ECHR). Since no federally protected right to privacy exists in the United States, there has been increased contention between states, technology companies, scholars, and citizens around how to protect consumers' privacy in digital spaces.

Hence, while the United States has seen some attempts to legislate privacy in both statutes and case law, most of these attempts at regulating personal privacy have

failed to effectively challenge the supremacy established by the First Amendment's freedom of the press. Yet, scholars, media, and movements within the United States show support for some measure of digital privacy among U.S. citizens. Bode & Jones (2018) found that 67% of U.S. citizens supported a right to be forgotten, and that support for a right to be forgotten transcended typical Democrat-Republican divides (Bode & Jones 2018, 253). Thus, while there appears to be growing support for a right to be forgotten or some other measures of ensuring digital privacy, the United States has seen slow, if not insignificant, movement on the right to be forgotten.

While the First Amendment has thus far posed significant barriers to digital privacy statutes, many pundits, scholars, and legislators have suggested alternative pathways towards protecting one's personal information online. In suggesting alternatives to the U.S. default of persisting digital remembrance, Leta-Jones (2016) suggests that creating a mechanism more in line with "U.S. forgiveness and information stewardship" could be implemented through digital addenda to existing search engine results that marks information as old or otherwise incorrect (p. 149). The idea behind this measure would be to implement a right to respond for individuals online by allowing that "information can be added to harmful content to provide context and accuracy" (Leta-Jones. 148). While this solution would allow some form of moving forward past transgression for individuals, Leta-Jones also discusses how this would leave a "mass of expired informational waste and would add conflicting information to the pile," such that adding context and accurate information may not offer enough relief from one's past (Ibid. 149).

Given the potential legal and social barriers to a right to be forgotten in the U.S., other scholars argue for different piecemeal approaches to digital privacy, or a more limited right to be forgotten, to be transplanted to the United States as well as to the rest of the world. Leta-Jones offers a potential solution via a narrower right to be forgotten, through "remixing false-light and retraction law" to make a viable right to digital oblivion in the United States (Leta-Jones 2016, 148). In contrast, Colgate Love (2003) argues for a path forward through rehabilitation and transformation, but instead extends the argument of rehabilitation through public reckoning, or a right of the individual to respond to information posted about them online. She argues that while pathways for expungement do not necessarily have to be adopted, there must be some form of systematic review of rehabilitation for formerly incarcerated people. While a society need not forget one's crimes and wrongdoings through sealing records or deleting them upon release from incarceration, there must be pathways for one to "restore to society's good graces" (Love 2003, 1709). Maruna (2011) continues this discussion of the value of public recognition and forgiveness as potentially necessary parts of rehabilitation. Rather than having a time-expiration or a passive expungement of information, Maruna argues that active rehabilitation through acknowledgement of wrongdoing serves to lessen consequences faced by offenders, and that "reintegration is a 'two-way street'" between an individual and the society they return to, such that a society must know one's past and still be able to forgive (Maruna 2011, 106). There must be some repentance by the individual who has done wrong or caused harm, but an equal recognition of such rehabilitation efforts and some kind of pathway back into society; otherwise, there is little

point to an individual trying to change their life, move on from past mistakes, or grow in any way. Thus, having a certification process—of both inaccurate or outdated information, or to mark one's progress beyond wrongdoing—allows for a public acknowledgement, acceptance, and ultimately forgiveness in both a social and legal context, without the same removal of information on the internet.

Given technology's progress and the generative environment of the internet, new technology will always outpace developments in regulation and legislation, and even the ethical frameworks that inform laws. With this growing "ethics gap" between technology and law, many scholars argue that existing laws in the United States are not flexible enough to accommodate the unforeseen circumstances and speed of development initiated by the digital age (Moor 1998, 16). Brock (2016) articulates that any reform for digital privacy will likely "distort the original purpose" of the law (Brock 2016, 34). Concerned with the potential effects of censorship on news media and mass communication, Brock argues that the right to be forgotten, as envisioned by the EU, will likely result in a culling of accurate information and the public's right to know. Given the asymmetry between digital advancement and the timeline for development of policy in response, Brock and others argue that the EU's right to be forgotten may over-develop consumer protections to cause widespread censorship of information. Brock argues that "data protection rebranded as the right to be forgotten, however well-intentioned, carries the risk of shrinking freedom of expression" (2016, p. 37).

Though the U.S. has resisted a right to be forgotten (or other measures of digital privacy), the future of the right in the United States still garners considerable

international and domestic debate. Why has the U.S. been slow to address digital privacy concerns, especially considering that certain dimensions of privacy have already been developed? Many scholars have explored the apparent contradiction of the right to be forgotten with existing First Amendment protections of freedom of speech. Frank Pasquale (2015) challenges this narrative of First Amendment supremacy in the United States by looking at existing laws protecting medical information and bankruptcy records and charters a path forward for legal reform around digital privacy. Pasquale contends that laws already exist to protect privacy in some contexts, namely concerning medical privacy; HIPAA rules prevent patient information from being released, and "internet providers can be held responsible" if data breaches happen (Pasquale 2016, 530). Similarly, the Fair Credit Reporting Act, the basic laws surrounding bankruptcy, outlines a delisting process for any bankruptcy after 10 years, intentionally building in a policy mechanism to allow a fresh start for people who otherwise would be unable to move on. These existing laws, Pasquale argues, assume that people who have gone through bankruptcy should be given a second chance and allowed to continue their participation in the economy once they have financially recovered from bankruptcy.

Though various scholars have explained the challenges and collateral consequences faced by individuals with criminal records and past convictions, and other scholars have explored the rapidly changing dimensions of the right to privacy in the digital age, there is a lack of research into how privacy rights could address the many issues plaguing people with arrest or conviction records and could redefine the rights of all citizens under the new digital regime. Criminal justice reform must clearly address the

gaps in regulation that allow criminal records to be published and republished, but how can a country's existing legal framework define the dimensions of progress for criminal justice reform online? In this study, I will explore the creation of a right to privacy before the digital age, existing legal and criminal frameworks around rehabilitation, and an exploration of case law in a two-case country comparison—France and the United States—in order to shed light on potential privacy reforms in the age of information.

Framework and Case Selection

Privacy has undergone a change in its meaning and scope in light of widespread availability of information online, coinciding with changes in the criminal justice system and larger questions on a statutory and regulatory level of what rights ought to be extended to citizens in the era of digital information. In each of the two country cases, France and the United States, there have been opposite approaches to digital privacy; in France, the adoption of a right to be forgotten, and in the U.S., a refusal to legislate on the issues of digital privacy. I have chosen France as a civil-law country exemplifying the protection of privacy in the digital age. While the initial right to be forgotten case was heard in the Spanish court (AEPD), France's data-protection agency (CNIL) has considerably expanded upon the right to be forgotten through active enforcement of the GDPR, being the most active with requests for deindexing information. Likewise, France also has comprehensive measures to ensure privacy for ex-offenders and to provide a pathway for desistance from crime. Given these robust privacy protections in France, coupled with rehabilitative criminal justice measures that allow individuals to move

beyond their transgressions, France offers an interesting corollary case for applying lessons learned in digital spaces to existing criminal justice systems.

In contrast, the United States shows how the common-law framework has proven less adaptable to emerging issues (such as the rapid development of technology), and the U.S. Constitution and statutory protections divide the right to privacy into different levels of protection. Coupled with punitive criminal justice systems, the right to privacy offers few mechanisms for forgetting one's past, especially for people with records of wrongdoing.

Using an inductive approach and thematic analysis of legal doctrines of privacy, I will draw observations from case law, legal culture and theories of privacy, and the specific legislative developments of the right to be forgotten. In looking at a country with more success in implementing digital privacy, I will identify patterns that could lead to potential policy channels for a right to digital privacy in the United States. I will also explore how existing legal frameworks and the punitive nature of a country's criminal justice system lend themselves to either more rehabilitative or more punitive digital privacy laws, in order to characterize whether adopting a "tough on crime" approach means a country will also be "tough on digital footprints." Each section of this thesis will focus on one of the country cases and will address the different historical and case-law underpinnings for privacy before and after the advent of the internet, the differences between a right to be forgotten in the civil versus criminal law contexts, and the cultural, legal, and political contexts of the countries in question.

Section III: France: A Model for Right to Be Forgotten Enforcement

While the first court cases that tested the right to be forgotten came out of Spain with *Google v. Spain (AEPD)*, much of the underlying framework for data privacy can be found in French court decisions leading up to the digital age. In this section, I highlight how France's existing legal culture, including its hybrid-civil law background on privacy tort law, paved the way for the digital right to privacy. Likewise, France's longstanding constitutional commitment to the citizen's right to privacy over the public's right to know allows the French government and data protection agencies to enact digital privacy policies and regulation more adeptly than other European nations or the United States.

A "Remarkably Uncivil" Introduction of the French Privacy Right

The ways countries confront wrongdoing and rehabilitation, as well as privacy, have been shaped by developments long before the digital age. The commitment to one's own information has long been considered a right granted to French citizens. Although it is now considered a firmly cemented right of the French citizen, the right to privacy, and the ability to control information about oneself, begins its journey not in the French Civil Code, as we might expect from a civil law country, but rather in the courts.

The Civil Code became France's first attempt to codify all the rights and responsibilities of the French citizen, following the philosophical traditions of building a legally enforceable social contract. Broadly, the Code defined property rights and the equality of all people under law. However, throughout the first iterations of the Civil Code going into the mid-19th century, there was still no explicit mention of privacy rights. Rather, the Code demonstrated the civil law tradition of codifying all human rights that one receives by virtue of living in a society and under the State. Some of the early

French rights protected by law included the rights to freely form thoughts (and express those thoughts), and property rights, with both of these rights finding ideological roots in the *Declaration on the Rights of Man and of the Citizen.* Reflecting the spirit of revolution and the fears of censorship by the government, the *Declaration on the Rights of Man* is laden with protections for the right to be able to "speak, write, and publish freely," in order to be an enfranchised citizen (*Declaration on the Rights of Man and of the Citizen, Article 11)*. This ability freely falls into the "moral rights" of the creator: that the product of one's writings and musings, one's very thoughts, are an intrinsic part of one's human nature (Hauch 1994, 1230). Connecting to an individual's rights as a citizen implies an understanding that one must have freedom of thought in order to freely engage in a democratic forum. If one cannot freely express themselves fully, they cannot be a functioning member of a democratic society. However, ascribing thoughts and ideas as a measure of personhood and citizenship alone does not provide adequate protection (or any sort of legally enforceable rule) to a person's right to privacy, and a right to control information about oneself.

However, the other component of state-building within the document is the concession of living in society. One must abnegate some rights in order to allow for society to function. In order to balance these two opposing truths, the *Declaration of the Rights of Man* articulates the idea of liberty of action, that "liberty consists in the freedom to do everything which injures no one else" (Article 4). This assertion that neither society nor government has control over an individual's personhood-building right to be left alone, except when they infringe upon another's rights and jurisdiction, allows much

more flexibility within French legislation and jurisprudence (Braxten-Craven 1976, 706). Although these protected rights—the ability to freely form thoughts and the "liberty" to do anything that does not harm another—do not entirely constitute a right to privacy, they become conflated with 'personality rights' by numerous French judicial decisions.

Beginning in the mid-1850s, new innovations occurred that allowed for people to capture likenesses more easily, and the boundary of what constituted one's property began to take on an amorphous dimension. In 1858, a case arose involving a reproduced and circulated sketch of a celebrity on their deathbed, which allowed the court to begin to develop the boundary of what counts as one's "property." A famous actress named Rachel was photographed on her deathbed by her family, with the photographer under strict orders to not publish or replicate the photos, yet sketches based off of these photos began circulating in the press. In the 1858 *Rachel* decision, the lower Tribunal Court (Tribunaux de Instance) ruled in favor of the plaintiff, resulting in the destruction of the artist's sketches and removal of any media (Beverly 2005, 147). The judge listed the "emotional damages" and violation of privacy as protected under Article 1382 of the Civil Code, which states that "any act whatsoever of man, which causes damage to another, obliges the one by whose fault it happened to repair it," and in the judge's ruling of this case, the moral damages caused to the family by leaking this photo amounted to enough harm that they demanded the image be destroyed (Hauch 1994, 1232). Thus, the judge interpreted the photo depicting a person, or any creative works that depict one's likeness, to be an indelible part of one's personhood in France.

While this may not seem revolutionary, the *Rachel* decision established the first instance of interpreting one's own image as an intrinsic part of what are now deemed 'personality rights.' Personality rights encompass all of the identity-forming and intellectual property dimensions of speech and of material creation, the qualities that are "attached to the person and cannot be waived or alienated" (Hauch 1994, 1230). Since the *Rachel* decision, the French courts have argued time and again that personality rights are intrinsic to an individual, and they are able to be extended and withdrawn only by their person. Thus, the ability to claim damages against infringement of one's personality "should be based, not on the rules of property, whether material or artistic, but on the right every human being has to have his personality respected" (Beverly 2005, 148). While no explicit links existed between personality and property rights, the courts established a strong connection between personality and ownership of one's likeness and one's ideas. In this landmark decision, the courts stretched the idea of the property rights of the family to encompass a reproduction of a photo, acknowledging that "the courts were left to deal with unforeseen situations and had to do so with the limited resources of the Code" (Bernard Audit 1978, 753).

This use of court decisions and case law precedent is notable because France, like many other European countries, draws its legal system from the civil law tradition, whereby the government uses "written reason" as the predominant method of deciding disputes (Radamaker 2002, 130). Thus, since the mid-1850s, French judges have been tasked with interpreting these broader rights articulated in the Civil Code in new and uncertain circumstances. Emerging technology, such as the daguerreotype (a predecessor

of the camera), were combined with existing laws in the Civil Code to almost demand that French judges play a more heavy-handed role than solely "applying the law" (Reichel 2007, 109). Courts were tasked with defining the extent of damages and whether one could seek legal recourse for what amounts today to invasion of privacy: "Without benefit of any legislative guidance on the subject, French judges essentially created the right to oppose the publication of private facts" (Hauch 1994, 1231). This legal precedent held for almost a century, where judges repeatedly followed this initial ruling to oppose disclosures of an individual's privacy. In these few hallmark cases involving "personality rights," courts had little legal framework in which to situate their decisions, and thus had to create judicial precedent in the absence of laws, such that "the right to one's name and the right to one's image are nevertheless firmly established in French law, notwithstanding their purely jurisprudential origin" (Beverly-Smith 2005, 153).

In addition to the *Rachel* decision, other cases emerged around personality rights in this era; the *Dietrich* case over a century later featured the release of true historical accounts of the life of German Actress Marlene Dietrich without her consent (*Marlene Dietrich v. Société France-Dimanche 1955, Cour d'Appel de Paris*). In accordance with the personality rights that the French judiciary has historically upheld, the appellate courts in Paris ordered *Société* to pay damages, claiming that "an individual's reminiscences of his private life form part of his moral capital," and that this fell under the purview of the existing rights to privacy and personality as laid out by former French case law (Markesinis 2009). Thus, French personality rights developed, in part, from an abnormal use of the judiciary system to set the boundary of personality rights as a

mixture of "property" and "liberty," which then became enumerated and codified into the French Civil Code.

Though the right to privacy drew its legitimacy from case law precedents, the legislative origin of French privacy rights connected to new developments of privacy across Europe, with the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1953, along with an explicit addition of a right to privacy in France in 1970. The French Parliament initiated new amendments to the Civil Code with Article 9, which enacted a broad right to require respect for one's privacy as a personality-forming right, such that "everyone has the right to respect for his or her private life" (Article 9, Civil Code). In addition to stating the relevant rights around one's private life, this article also established an action plan for violations of one's private life, including a section in the Criminal Code set aside for individuals who violate another's right to privacy (Deringer 2003, 196). On one hand, for more minor information releases, the plaintiff can sue for damages; on the other hand, for major violations of privacy, one can ask for a total injunction of the information (Hauch 1994, 1242). Therefore, while judges still play an active role in the enforcement of the right to privacy, the right has become firmly cemented in French culture, such that invasions of privacy become a violation not only of social and cultural norms, but of law as well. With this legislative push behind privacy rights, the right to privacy in France moved from an implicit, judicial precedent towards an explicit, constitutionally protected right.

Rehabilitation and Desistance through Privacy

In France, the right to privacy has been enacted through legal codification and judicial policymaking, such that individuals have the ability to prevent personal information from becoming public. However, does this right also apply to individuals in France with records of incarceration? Another key takeaway for the French laws on privacy, and specifically moving towards digital privacy, are the implications for the criminal justice system. In France, the criminal justice system maintains comprehensive records of arrest, conviction, and imprisonment on its population. In contrast with the U.S. system where records are considered public information, criminal records of French citizens cannot be accessed by the general public, except for in narrow circumstances where an individual's employment may put them into contact with vulnerable populations (children, e.g.). Privacy and respect for every person's dignity has been a prominent feature of the French criminal justice system, which translates to people convicted of wrongdoing. In implementing privacy through criminal record expungement, the French judiciary engages in the practice of 'judicial rehabilitation,' which is designed to show society that an individual is actively participating in transformation after their actions of wrongdoing.

Information about criminal records is considered extremely sensitive by the French government, and these records are legally only allowed to be stored by the National Judicial Record (NJR), a national database established for maintaining records of all French citizens. Article 777 of the French Criminal Code lays out the regulations around reporting and publishing criminal records in France (Act no. 70-663, Criminal Code). Under these regulations, an individual's criminal history is classified as sensitive

information only available to government administrators in most cases, and by the individual seeking their own criminal record in others. The organization of records follows a delineation of histories of criminal offenses into three categories, known as bulletins. The 1° bulletin is reserved for administrators within the NJR, unable to be accessed by anyone outside of the criminal justice suite (Article 774-1, Criminal Code). The 2° bulletin allows for certain governmental authorities to see an individual's record of felonies or misdemeanors in the case of the individual seeking "public employment, joining the military, filing in bankruptcy courts, or engaging in any public or private enterprise with cultural, educational, or social activity with minors" (Article 776). However, numerous exceptions exist for information on the 2° bulletin; for example, where sentences under 5 years are automatically removed after a time, or are excluded from the record by the judge's orders either at the time of conviction or after the sentence has been served (Article 775-11). Lastly, the 3° bulletin reflects an individual's criminal record for felonies and misdemeanors which are not excluded from the 2° bulletin, such as in the case that the individual may have habitual volunteer or professional exposure to minors in their jobs (Article 777). Thus, the access to information about an individual's past wrongdoing has a system of checks to make sure that past criminal records are only accessed on a need-to-know basis.

As Herzog-Evans explains, access to an individual's criminal records is protected to ensure that the courts—and by extension, the records of criminal wrongdoing that the courts create and maintain—do not jeopardize an individual's attempts to reintegrate into society after conviction. The goal of crime prevention "precisely requires for the person

to have social and human capital," which translates to the ability to socialize oneself back into society through work, housing, and structures which help reintegration (Herzog-Evans 2011, 7). The goals of the French criminal justice system are to encourage individuals to engage in prosocial behavior and to hopefully prevent return into the prison system, so France's criminal code supports this mission by providing much more stringent rules around reporting of criminal records. Thus, the goal of society is to uphold a culture of forgiveness through selective informational awareness.

Given this, the various bulletin processes serve as a first-order control over who can see an individual's record of wrongdoing, with the different levels of accessibility allowing an individual to have a better chance of moving on post-transgression. Although Herzog-Evans does describe instances of employers in high-trust industries (banks, working with children) needing access to an individual's record, the highest French Court (*Cour de Cassation*) ruled that an individual does not have to share their criminal record with employers in most cases, which has cemented French jurisprudence as part of a "desistance-friendly" culture (Ibid. 8). So, the French legislation under the Criminal Penal Code and the High Court have both embraced the mindset that a potential answer to criminal wrongdoing is to engage in active reintegration as a form of recidivism prevention.

The three main mechanisms of record expungement in France are automatic deletion, legal rehabilitation, and merit-based judicial rehabilitation (Herzog-Evans 2011, 11). Automatic deletions occur after a certain period of time, without any input from the individual. Usually, this passive process occurs after 40 years, and again at 100 years, if

an individual is still alive, in order to demonstrate goodwill towards the elderly (Maruna 2011, 101). Legal rehabilitation also occurs after a period of time and occurs when an individual has remained "crime-free" for that time after release (Ibid. 98). In contrast to both of these more passive, time-tracked processes, France also has an active participation process under judicial rehabilitation, which allows an individual to demonstrate an "honor roll" status after their sentence where they have both desisted from crimes, made amends to the victims of their actions, engaged in visible displays of rehabilitation, taken accountability for one's previous actions; they can then be eligible for a judge to clear their record from the 2° and 3° bulletins (Herzog-Evans 2011, 13-14). This process is regarded very seriously within the France judicial system, whereby an ex-offender is examined in every instance of their time since conviction, to observe whether they are "truly a desister" (Ibid. 15). This use of judicial rehabilitation reflects the solemnity inherent in certifying the rehabilitation of an individual before wiping one's slate clean, but it also builds in a model for allowing forgiveness and forgetfulness to extend to one's past.

While these processes for record expungement do exhibit considerable concordance with the right to privacy in France, they also serve to recognize the importance of public reckoning with criminal justice and the ripples of harm caused by transgression within one's broader community. Recognizing both the harms caused by the individual and the performance of stigma throughout conviction processes, judicial rehabilitation stands to ameliorate the social, emotional, and economic consequences of having a criminal past. Not only does this serve as a personal emblem of transformation

for the ex-offender, but more importantly, it serves as a symbol to the community and people surrounding the ex-offender (Maruns 2011, 109). As the French case demonstrates, an individual's right to privacy (especially in terms of criminal records) can still be preserved while also acknowledging one's past actions, through having a judicially supervised process which balances both the right to privacy of one individual and the right to *see* that a person has actually engaged in rehabilitation.

While the stated goal of French imprisonment is to rehabilitate individuals, and to have the punishment be done upon release from prison, there are still some limits to one 'wiping their record clean.' Judicial rehabilitation is not available to every ex-offender, and crimes of sexual violence and harm against children are ineligible for removal. In contrast to pathways for judicial rehabilitation, people convicted of sexual offenses must enroll in the NJR's database for Sexual Offenders, which codifies a process for communicating an individual's sexual offender status to relevant local authorities, such as reporting any changes of address to police (National Judicial Record for Sexual and Violent Offenders). However, this database is still only accessible by relevant authorities, and when an ex-offender may work or volunteer with vulnerable populations, so it does not form as serious a barrier to an individual's return to society as in other countries' laws around sexual offenses (for example, SORNA laws in the United States, which can require an individual to notify one's community, not solely law enforcement) (Herzog-Evans 2011, 8). In recognizing the causes of recidivism, French criminal justice records for even the most serious sexual offense crimes are still kept private in an attempt to

distance an individual from their previous acts of harm, and to prevent further acts of crime.

Privacy as a Fundamental, yet Relative Right

Privacy has remained an indelible part of the legal rights of French citizens, whether in photographs of an individual, written accounts, or in digital spaces. Although the entirety of the GDPR, the Civil Code in France, and the assertion of the right to privacy in the European Convention on Human Rights (Article 8) all delineate the bounds of the right to privacy afforded to French citizens, the right to privacy still exists in tension with the freedom of expression. The French Parliament incorporated a right to expression into the 1881 Freedom of the Press Law. However, the French right to expression will likely be unusual to U.S. audiences, given that it also recognizes the potential violations that can occur at the hands of the press, and in the name of public interest.

Thus, while the right to press is still enshrined in the French Civil Code, the right to publish information has limits; that is, freedom of expression is not an absolute right. While the right to privacy protects a person's dignity, access to information promotes democracy and the transfer of ideas, with "the internet play[ing] an important role in enhancing the public's access to news," thus serving as a vital check on democracy (Kulk and Borgesius 2017, 9). The Civil Code acknowledges both the right of others to know information about us and the right to one's privacy, such that the right to expression and the right to privacy are weighted equally.

While foundational revolutionary texts reflect the need for freedom of expression to serve as a vital component of democracy in France, the right to expression is not viewed in a vacuum. Rather, an individual's right to privacy must temper the 'right to know' in France, such that the freedom of expression is constrained much more readily than the U.S. French laws and authorities air on the side of protecting an individual's right to privacy, unless in cases of public interest. France still maintains a strong right to freedom of expression under Article 11, yet this ability to "speak, write, and print with freedom" becomes tempered by the content that it contains; an individual is held accountable for their speech when it infringes upon the rights of another (Article 11, Declaration of the Rights of Man and of the Citizen).

This protection of a right to privacy can be seen in how individuals in the public's interest (be they celebrities or politicians) are able to sue for invasion of privacy. While interesting gossip about celebrities or embarrassing photos of politicians may be considered public domain elsewhere, France's privacy protections demonstrate that the right to privacy trumps the public's right to know, *except* in cases when an individual's private life has been seen to "cause" the public incident. Celebrity status alone does not meet that threshold for newsworthiness. In the 1996 case involving the inviolate personality protection of all people under French law, the *Sachs* decision involved republication of known information about a celebrity. In the *Sachs* case, a famous German playboy sued after *Lui*, a French newspaper, published an article about his life. While most of the information in this publication was already in the public record, the Cour de Cassation, the highest court in France, declared that the prior consent of an

individual in publication does not translate to the media being able to republish information. That is, "prior cooperation does not create a presumption that he would permit any magazine to assemble and reproduce" information about the decision (Palmer 2020, 265). Even individuals who profit from their public image are entitled to considerable protection of their personal lives in France; courts recognize that even celebrities have a private life away from the public eye.

Given the well-defined right to privacy for all citizens in France, it is no surprise that celebrities remain protected from public scrutiny in many disputes about privacy. And, the widespread protection of privacy as an innate personality right attaches itself to people, not places, to allow for celebrities (and other individuals) to control their image *even* when in public spaces.

Privacy into the Digital Age

While both the 1858 *Rachel* decision and the 1970 addition of Article 9 into the Civil Code created the right for privacy within France, French legislators took a proactive approach to looking at the effects of the internet on enforcing French privacy law. As early as 1978, the French Parliament passed Act no.78-17 of 6 January 1978, "On Data Processing, Data Files and Individual Liberties." This French Data Privacy Law laid out the continuation of French rights into the digital world, such that the "data processing shall be at the service of every citizen" (Section 1, Act 78-17). Notably, this information technology law laid the groundwork for the right to claim personal data as an extension of one's private life. The law expresses the need for widespread access to technology, yet access that "must not infringe human identity, human rights, privacy, or individual or

public freedoms" (Article 1, 78-17). Thus, the French legislature implemented policies to allow for a continuation of the already-established privacy rights of the individual to be translated into the digital realm.

In addition to setting up the early case for digital privacy, the 1978 law also established the National Commission for Information Technology and Civil Liberties (CNIL), the French data protection agency. This Data Privacy Law, and the powers granted to the data protection agency, have since been updated in 2000, 2004, and finally in 2016, such that the latest version states that any French data subject has the right to control information about one's self, to "correct, complete, update, or delete personal data" if it is deemed inaccurate, incomplete or out-of-date (Article 40). Today, the CNIL is the French regulation agency responsible for pursuing data privacy complaints, and for enforcing search engines to comply with the terms laid out in the EU-wide General Data Protection Regulation (GDPR). Thus, the French government has both worked in tandem with the EU's broader data protection through the establishment of the GDPR, yet they have also developed a separate body of legislation to enforce and codify the French citizen's rights to privacy in the face of changing digital technology.

The Road to the GDPR

The first right to be forgotten case was heard in Spain with *Google v. Spain* in 2014. The EU-wide appellate court, known as the Court of Justice for the European Justice (CJEU), heard the appeal, which allowed for the right to be forgotten to become an embedded process for residents of the European Union under the 2018 General Data Protection Regulation (GDPR) codification. While the right to erasure has become a

standard for all member states of the EU, data privacy protection in France draws credibility from a history of robust personal privacy, as well as movement toward data protection and regulation before the GDPR was enacted in 2018.

In the *Google v. Spain* decision, the plaintiff referenced a violation of the 1995 Data Privacy Directive and his right to control his own data around a home foreclosure. The DPD allowed for the "right to privacy with regard to personal data" (Directive 95/46/EC). This provided the initial legal basis for subjects to control the processing of their personal data online, and it hinged upon the role of data controllers and processors, like Google, and the extent to which they can elevate or lower certain search results.

Upon hearing this case, the CJEU ruled in favor of the plaintiff, Mario Costeja Gonzales, who was able to petition Google for removal of information about his personal history. The CJEU extended this reasoning further, to argue that search engines must remove—upon request—any information that one deems inadequate, irrelevant or no longer relevant, or excessive" (Xue 2016, 389). Given the implications across the EU for this interpretation of the 1995 Data Protection Directive, further developments resulted in the formal codification of the General Data Protection Regulation (GDPR) in 2016, which would be rolled-out over a two-year period, beginning in 2018. The General Data Protection Regulation's legal charter doubled down on the EU's commitment to the rights of digital privacy for citizens: "the protection of natural persons in relation to the processing of personal data is a fundamental right" (Regulation EU 2016/679).

Under the GDPR, the European Union allows the right to erasure to be applied in all member states, without each individual country needing to specify a law on the right

to be forgotten. Standardizing the procedure for the right to be forgotten streamlines the policy in two ways; one, it lowers the transaction costs between states when "condensing the informational and redemptive strategies" for both search engines and governments to enforce the right to be forgotten and delist results, and two, it provides all of the EU states with the power of collective bargaining (Leta-Jones 2016, 166). While the GDPR extended the right to be forgotten to the EU as a whole, the "interpretation and enforcement" of the data protection guidelines still remains a power of individual agencies (GDPR 2018).

The CJEU and the final GDPR legislation left the specific balancing of the right to privacy and the right to expression up to each Member State: "The GDPR text itself seems to retain elements of a directive with specific delegations of responsibilities to Member States to enact enabling laws" (Klinefelter-Wrigley 2021, 727). Hence, the preference for respecting an individual's right to privacy over the community's right to know—particularly in France—is evident; the 2018 GDPR law created a well-defined right to control one's own data as well as the means to petition for removal of any information (Articles 15 and 17, GDPR). While the courts and the legislation both asserted that an individual retains a proprietary ability to control information about themselves online, they also assert that this right does not exist in isolation. Rather, the digital privacy of the individual must be balanced against the public's right to know. That is, "the judgment vigorously made it clear that none of the competing interests, in particular, individual privacy right and public freedom of expression are exclusive, therefore, both of them can be restricted, if appropriate reasons are found reconciled

within the law" (Faisal 2021, 7). Thus, in the EU, neither the individual's right to privacy nor the right to expression is absolute. Likewise, the GDPR allows for individuals to petition data controllers for removal of certain links to sources on a specific site, while the process for complete removal of the information from the internet as a whole would require a separate request, such that the "display of a link in search results must be considered separately from the initial publication of the information" (Globocnik 2020, 380). However, the burden of proof for whether something counts as within the public's purview more often than not tips towards the individual's right to privacy.

France's Eager Adoption of the 2018 GDPR

With the passage of the GDPR, the right to be forgotten has since become ingrained into French civil rights and serves as a signal of the French commitment to the right to privacy in digital spaces. Although the 'right to delete' was first enacted for the entire EU in 2018, the French legislature began developing legislation that would eventually support the French right to be forgotten decades earlier. While the origins of digital privacy for the broader EU date back to the 1995 EU-wide Data Protection Directive, France had already established its eminence within the field of digital protection for citizens in 1978 with the French Data Protection Act (Act n°78-17 of January 6, 1978). Indeed, this early adoption of privacy rights has set the standard for France to be a model adopter of the General Data Protection Regulation (GDPR). Likewise, given France's early adoption of digital privacy into the Civil Code, it should come as no surprise that French legislators sought to codify digital privacy above and beyond the EU right to be forgotten policy. While the EU-wide GDPR was implemented

in Regulation (EU) 2016/679 to go into effect in 2018, the French Parliament passed a separate bill, Law n° 2018-493, known colloquially as "The French GDPR Law," which amended the existing 1978 Data Privacy Act to better reflect the evolving language of internet privacy, as established in the GDPR. This 2018 law amended the 1978 Data Protection Law to exhibit concordance with the GDPR, but also went beyond some of the regulatory guidelines established in the GDPR. Some of these requirements under French law stress the ability for an individual to find out what kinds of personal data exists about them, as well as key recommendations to data controllers (internet providers, search engines, and other large technology companies) on how they can best meet the standards laid out by the French GDPR Law. This allows for participation from tech companies in the process of data regulation; CNIL not only encourages the development of codes of conduct and new ethical standards, but it allows for interface between the governmental regulators and key industry players. Under the amended law, CNIL has been granted additional legislative power in order to actually challenge and regulate in the face of massive corporate interests. This includes protecting people without much digital literacy (Section 1, Law n° 2018-493), as well as individuals with criminal records, medical information, and all other extremely sensitive information that could face additional risks by virtue of immediate access to the internet. Thus, the prior legislative steps taken by the French Parliament on properly assessing the new benefits, and risks, of technology allowed CNIL to take an early lead on digital privacy across the European Union.

CNIL has been active in their oversight of the right to be forgotten; the process of the right to petition for deletion first goes through Google, or other public search engines

deemed “data controllers” under the GDPR’s guidelines. For example, if Google refuses to delist the petitioner’s request, the individual can then appeal this decision either to the EU-member country’s courts or to the country’s data protection agency. CNIL has, for example, challenged Google’s attempts to limit the right to deletion to only EU countries, arguing that the right to delete applies to all French citizens, regardless of their location. In 2014, CNIL’s lead regulator argued for the right to be forgotten to be applied globally, given that search engines are legally required to remove information after the petitioning process in select jurisdictions but do not necessarily need to delist information in other locations (for example, one could find an article on Google.com that was delisted in Google.fr) (Satariano 2019, NYT). Regulators in France reasoned that a delisted article’s reappearance in another country effectively “circumvented EU law,” and thus decided to outline a written basis for compelling search engines to de-list information outside of national domains (Article 29, Data Protection Working Party). However, Google appealed this new ruling from the French regulators, arguing that requiring delisting of links across the entire Google suite would amount to censorship for all non-French internet users. The regulation actions were eventually declared unconstitutional by the CJEU in 2019, which ruled against the data protection agency and this territorial extension of the right to be forgotten (Marsh 2019). Even though the French data protection regulators lost this appeal about the territorial limits of the right to be forgotten across all of Google’s country domains, the right to be forgotten still applies to the 28 Member States of the European Union.

Considering the CJEU's judicial curbing of CNIL's authority, many important interpretations of the right to be forgotten are still in development in France. In the past two cycles of review of the right to be forgotten, which occurred in 2014 and 2020, the French data protection authority has overseen an exponential increase in people visiting the CNIL webpage, and a large number of right-to-delete requests (CNIL Activity Report 2020). If the request for delisting is not approved by Google (because the information is in the public interest, or the request does not meet the "outdated" standard or is otherwise not treated with "undue delay"), then individuals can file a formal complaint with CNIL. In 2014, CNIL received 5,825 complaints from individuals around Google's deliberations on right to delete cases (2014 Activity Report). In 2020, CNIL received 13,585 complaints from French citizens against search engines, marking a 62% increase since the implementation of the GDPR in 2018 (CNIL Activity Report 2020). The French data protection agency has celebrated this continued use of the GDPR by the French citizenry, as it demonstrates the integration of the right to be forgotten into the French legal doctrine as an important right.

Criminal Records and the Right to Be Forgotten

Given the importance of the new digital privacy rights under the GDPR, the issue of weighing the right to privacy against the broader public's right to freedom of expression calls into question the fundamental role of the right to be forgotten. Criminal records represent one major area instance where an individuals' right to be delisted challenges notions of information that *should* be available to the public.

Often, individuals who have been convicted of a crime become unwilling participants in the news media, flung into the public eye by virtue of their crimes. Although their crimes may attract public attention, the legislation in the GDPR allows for delisting of unsavory past convictions and links to news stories since these convictions may not be serving a "newsworthy, journalistic, or literary purpose" within the public domain, especially considering a time-expiration component of information becoming outdated over time (Faisal 2021, 8). So long as an individual no longer retains relevance to the public, the information can be delisted. Individuals' reputations could be jeopardized by information freely circulating online, so the enforcement of the right to be forgotten also serves to ensure that an individual can move beyond their transgressions.

Publication of a person's criminal record, or allusions to their past history of wrongdoing in newspapers, could also crush the "embryo" of socialization that many ex-offenders need in order to regain social capital and rebuild their lives (Herzog-Evans 2011, 7). Legislators in France recognize that community plays a monumental role in criminal justice spheres, with that role being a boon to an individual's reentry into society, where the smallest shred of prosocial activity must be honored and encouraged to grow. Thus, the EU's right to be forgotten chooses a higher standard for information to remain in the public interest; rather than focusing on "whether a piece of information was right or wrong, the EU's legal system draws focus to whether the processor of the data has the right to reveal the information or not" (Faisal 2021, 9). The truthfulness of the past conviction plays no role in determining whether to publish information against an individual's wishes to keep it private. The only exception to this privacy regarding

criminal records comes into play if an individual chooses to work in roles that require particular sensitivity, or interaction with children, for example. Thus, the data processor has a right to reveal information about past wrongdoing *only if* an individual continues to seek high-trust positions, for example, or wishes to continue working with vulnerable populations, and *if* their conviction is related to their post-conviction current circumstances. Faisal (2021) offers the case of a teacher who abused their post in order to commit fraud, and after serving their punishment, attempted to return to work in a school as an entry-level employee (Ibid. 8). This individual would have a much harder time seeking delisting from search engines than an individual who returned to a quieter life further from the public eye. In accordance with this weighing of the public interest in an individual's past criminal convictions, the GDPR adopted Article 10, which allows for the delisting of information related to an individual's criminal past, and returns the control of criminal convictions to the relevant authorities of the Member States (Art. 10 GDPR). This ensures that the GDPR exhibits concordance with the existing Criminal Code of a country and allows for an individual to effectively move beyond histories of transgression and to regain society's good graces.

The right to be forgotten, then, is as much about weighing the public's right to know information about an individual as it is about protecting citizens' right to privacy online. Rather than inventing law, the right to be forgotten derives from the EU's individual right to privacy that predated the digital age. In allowing for technological and legal adaptations around privacy, France and the EU assert that the right to be forgotten serves a "fundamental need of an individual to determine the development of his life in

an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past, especially when these events occurred many years ago" (Mantelero 2013, 2). While prior to the internet's existence, individuals could experience reputational damage through private information being made public, digital spaces greatly expands the circulation and permanence of information, so forgetting and moving beyond transgression can become nearly impossible. Thus, courts and the legislature in France—already familiar with striking the balance between the public's right to know and the individual's right to privacy—created an ability to allow for selective, yet intentional, forgetting of personal information. The only new factor initiated by the right to be forgotten is to extend existing laws into the digital sphere.

Second, these processes of information removal occur in tandem with existing policies towards expungement in France. One could go through the ritual of judicial rehabilitation before the advent of the internet, certifying to the courts and their community that they are rehabilitated (Maruna 2011, 102). However, this ritual would ring hollow if an individual's entire history of wrongdoing were accessible in news articles, and the mechanisms of expungement would not deliver on their promises to recertify an individual of their former status in society. Thus, the right to be forgotten works together with existing criminal justice reforms to allow individuals to actually allow an individual to move beyond one's transgression.

This section on France demonstrates how the right to privacy became a foundational, well-protected tenet under French law under Article 9 of the Civil Code,

and later across the whole European Union with Article 8 of the Fundamental Charter on Human Rights. Despite this origin of privacy as a personality right in the judicial system, the right to personhood traces back to the fundamental provisions of rights in the *Declaration of the Rights of Man and of the Citizen*, written in 1789. Because the right to privacy applies to all citizens under the law, both celebrities and people who have committed criminal offenses are still constitutionally granted the right to privacy. This universal protection of privacy allows for the law to deliver on forgiveness and forgetting of an individual's past, such that society need not carry the mantle of punishment far beyond an individual's transgressions. Likewise, the right to privacy has become even more entrenched into French law in the digital age. Given this early adoption of a right to privacy in France, the combination of judicial decisions and legislation allowed for a more streamlined translation of the right to privacy into the digital realm.

Section IV: The United States, Three Privacies in U.S. Jurisprudence

While the right to be forgotten passed as EU law with the ratification of the General Data Protection Regulation in 2018, there have been no federal laws—and little action on the state level—around the right to digital privacy. Why hasn't the 'right to be forgotten' taken root in the United States, and does it matter whether individuals have a right to control information about themselves? Given the potential personality-building components of privacy, the far-reaching consequences of abundant information, and the compounded barriers to rehabilitation for formerly incarcerated individuals and individuals with records, the United States' approach to privacy merits discussion, as do

the harms of the continued lack of legislation on matters of privacy. The United States has neglected to explore online privacy reforms in both civil and criminal contexts.

Following the creation of the right to be forgotten in the European Union in 2014, and the codification of the right to delete in the 2018 General Data Protection Regulation (GDPR), scholars, news outlets, and jurists in the United States approached the issue of digital privacy with varied degrees of enthusiasm. While one camp favors free speech and freedom of expression, decrying the right to delete as media censorship, others noted how the right to be forgotten in Europe could potentially pave the way for a similar right in the United States, albeit one that factors in different legal and social norms around privacy and data. However, due to the First Amendment right to freedom of expression, as well as countless precedent-setting court cases, unified digital-privacy measures face increasingly unfriendly conditions in the United States. To understand the steps taken thus far by the United States to address the issues of digital privacy, one must first begin with the history of the right to privacy in the U.S. more broadly. This section will outline the common law baseline of the United States, our relevant legal history of the right to privacy, existing norms around privacy in the United States, and the fragmented legal environment around privacy in the digital age.

Three Privacies in U.S. Jurisprudence

The idea that the common law can be rapidly altered, and the sense that it allowed for flexibility in unforeseen circumstances, is one that appealed to early developers of U.S. privacy theory. Warren and Brandeis attempted to build a civil right to privacy out of reputational harm, which ultimately proved to be an unsuccessful legal argument.

Likewise, William Prosser returned to the privacy tort in his 1960 *Privacy* article, which has since become widely accepted as the doctrine of civil liability for privacy. A confusing judicial landscape, coupled with narrowly defined privacy rights in certain domains (healthcare, education, etc.), has prevented the development of a comprehensive right to privacy in the United States, instead allowing a multivalent understanding of privacy to develop. Moving into the digital age, privacy protections for U.S. computer users have stagnated, and the federal government has largely left states to dictate digital privacy laws for themselves.

In contrast to the construction of privacy in France, where privacy directly encourages the development of an individual's personality, the United States has seen a lackluster embrace of privacy as a fundamental right of the person. Compared to the streamlined approach in France, which anchors privacy in a person's fundamental liberty to do anything that does not cause harm to another person under the *Declaration of the Rights of Man*, the United States' foundational legal doctrine leads to a heavily fragmented legal environment for the right to privacy. Fourth Amendment protections for the "right to be secure in one's persons, houses, papers, and effects" have been thoroughly developed through *Katz v. United States*, *Griswold v. Connecticut*, and even *Roe v. Wade*, to protect citizens from governmental intrusion (U.S. Constitution, Fourth Amendment). However, this same standard protecting against invasions of privacy is less developed in civil liability cases. The Supreme Court, in its "people, not places" creation of a reasonable expectation of privacy, simultaneously upheld that U.S. citizens have no general Constitutional right to privacy. Thus, the right to privacy has been bifurcated into

separate issues depending on whether the matter concerns civil versus criminal cases. Likewise, statutory protections exist for limited rights to privacy in select circumstances where the government has been able to regulate certain industries. The Privacy Act of 1974 controls how governmental agencies process personal information, the Fair Credit Reporting Act (FRCA) allows for the intentional forgetting of past credit violations to allow individuals another attempt at economic gains, FERPA (the Family Educational Rights and Privacy Act) protects the privacy of students and their educational records, HIPAA (the Health Insurance Portability and Accountability Act) developed protection for patient's health records, and COPPA (the Children's Online Privacy Protection Rule) monitors websites that are directed towards children aged 13 or younger.

Yet, despite all of these statutes that either directly address citizen's privacy or allude to the need for privacy rights in certain circumstances, the right to privacy in the United States has remained separated into the two categories of criminal and civil liability. Namely, individuals have a right to privacy in criminal matters to protect from incrimination of an individual from searches performed by the government, and a much lesser privacy right in the civil context. Why hasn't the United States embraced a unified right to privacy, and where do the relevant constructions of privacy in the United States originate? In this section, I will argue that the multimodal construction of privacy in the United States has created gaps in a unified understanding, and legally protected version, of privacy.

Common Law Underpinnings of Privacy

Following the Enlightenment ideals originating out of Europe, U.S. philosophers and political theorists similarly interrogated the relationship between propertied men and the government, and the natural, irrevocable rights granted to all people by virtue of being human. These "natural rights" became foundational tenets that the new U.S. government aimed to protect. Namely, the United States defined a limited government, tasked with protecting an individual's access to "life, liberty, and pursuit of happiness" (U.S. Declaration of Independence). In addition, the U.S. Constitution expanded the basic civil rights and liberties of the U.S. citizenry in similar fashion: government, particularly at the federal level, was seen as an antagonistic obstacle to the free flourishing of individuals.

Antagonism against the government can be seen in the negative construction of rights within the Bill of Rights, the ten foundational civil rights embodied in the first iteration of the Constitution. In the First Amendment, the rights to freedom of expression, speech, and press were laid out: "Congress shall make no law...prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press etc." (U.S. Constitution). In the U.S. context, the writers of the Constitution feared the abuses and overreach of government into individuals' personal lives. Rather than viewing the government as a potential guarantor of rights, the U.S. government served as the biggest threat to an individual's ability to engage in self-determinative activity, such as freely expressing one's thoughts to the public, engaging in protest or redress, or protecting one's own home from intrusions from government.

Given the limited civil liberties in the Bill of Rights, no single defined right to privacy exists for U.S. citizens and residents. Rather, the right to privacy has been constructed in bits and pieces of legal decisions, outlining the physical boundaries to which one's sanctity of space, body, and mind extends; often, the judicial interpretation of cases becomes decided entirely against an individual's right to privacy. The right most approximate to privacy occurs in the Fourth Amendment's right to property, protecting against "unreasonable searches and seizures," and being "secure in their persons, houses, papers, and effects" (Fourth Amendment, U.S. Constitution). Yet neither statutes nor Constitutional guarantees mention any protection for privacy; while the legal interpretation of the Fourth Amendment's right to privacy demonstrates a commitment to preserving one's privacy when it pertains to physical property inside one's home, this right does not extend to one's image or other characteristic components of identity.

The limited rights laid out by the U.S. Constitution reflect the legal design of many common-law countries. Legislators in the United States derive statutes, however, the Constitution has formed the legal backing for the creation of most legislation and case law precedent in the United States. Rather than articulating an entire civil code for every foreseeable right and need of its citizenry, common law frameworks rely on "development of law by a system of judicial precedent," such that all written laws derive their legitimacy from successfully being argued in the courts (Stone 1936, 5). Common law countries, therefore, attempt to assure that laws at local, state, and federal levels exhibit concordance with the Constitution. This process within common law countries, known as judicial review, has granted the courts the ability to "not only interpret, but

make the law" (Holland 1988, 21). In comparison to civil-law countries, the flow of legislation in common law countries is a much more involved process. Constructing laws relies first on the forming of legislation in the legislative branch, then moves on to the courts to engage in policy approval and demanding enforcement of legislation, while civil law countries need only pass Parliament for laws to join the main body of law in a country (with some exceptions around similar mechanisms of judicial approval).

However, the common law system does not create law in a vacuum. Rather, every judicial interpretation derives legitimacy in each ruling from a commitment to upholding existing legal precedent. While this does create conditions where the law is slightly imprecise and may not be perfectly applicable to new circumstances, connecting the current law to past law creates a trail of legal thought that allows interpretations to derive legitimacy from what came before. The process of judicial review, then, allows for re-imagining of old laws into new circumstances, so the law can potentially become more adaptable to the unknown.

Warren and Brandeis: An Unsuccessful Argument for Privacy

The adaptability of the common law may exist more in theory than in practice. While Warren and Brandeis praise the "eternal youth" of the common law, Palmer and other legal historians argue for the much more "glacial" course of the common law to effect change slowly, rather than with sudden creations of new rights (Warren and Brandeis 1890, 195 & Palmer 2011, 79). Still, early ruminations on a right to privacy in the United States have drawn on this potential for flexibility of the common law to deal with unforeseen circumstances in light of continuing advancement and pace of

technological gains. In 1890, Samuel Warren and Louis Brandeis co-authored a privacy tort "On The Right to Privacy." They aimed to clarify the legal and Constitutional basis for protecting a right to privacy, and they provide a pathway for a "right to be let alone" that is very in-line with contemporary European standards of privacy.

The "beautiful capacity for growth which characterizes the common law" inspired Warren and Brandeis to imagine rapid evolution of a new right to the un-litigated frontier of personality and privacy (Warren and Brandeis 1890, 135). Since existing U.S. Constitutional protections and statutes failed to anticipate the increasing intrusions upon privacy, Warren and Brandeis imagined the common law of the United States to be expandable to encapsulate new personality rights. Similar to how the *Rachel* Decision in France connected an individual's right to privacy to the sanctity of privacy as a personality-building domain, Warren and Brandeis address the "tangible and intangible" components of property to fully define privacy as a necessary component of an individual's personality rights (Ibid. 194).

Privacy was as much a protection of one's physical space against unwanted intrusions as it was protecting one's ability to freely think and develop one's "sensations and intense intellectual and emotional life," free from the prying eyes of media, government, or other citizens (Ibid. 195).

While the actions of individuals in the public eye (as celebrities, politicians, and other public figures are) can sometimes blend the distinctions between "newsworthy" information and tabloid speculation, the fundamental premise of the Warren and Brandeis tort is to argue that when an invasion of privacy occurs, an individual has the civil right to

pursue emotional damages. Protecting true, yet highly personal information from media sensationalization rests on the "damage to reputation," one's public image and interpersonal relationships become jeopardized by virtue of having private information made public (Ibid. 197). Drawing on a similar logic of reputation and honor that was becoming popular abroad, Warren and Brandeis argue that the emotional harms caused by publishing private information has a legal basis in historical systems of honor that have protected an individual against slights upon their character. Warren and Brandeis draw the right to privacy, beyond property and copyright law, to protect the essence of the individual to express thoughts without fear of encroachment.

For mapping out the boundaries of a right to privacy, Warren and Brandeis offer the idea of property as a better legal basis for privacy. Despite similarities to existing copyright law that protects creative works, Warren and Brandeis discussed how private writings, letters, drawings, or other personal musings do not fall under copyright law, since there would be no intent to publish. When private material becomes published without the consent of the author, Warren and Brandeis point to the creation of personhood as an intangible component of property as the basis for redress. Included in their definition of property, both physical space and intangible components of personality come together to form "the principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality" (Ibid. 205). Privacy forms an intangible component of personhood, extending beyond one's home or physical space to one's thoughts and feelings.

While Warren and Brandeis lay out this argument for privacy as a personality right and as intangible property, their argument also acknowledges that the right to privacy is not an absolute. Often, the right to privacy will conflict with the public's right to know. In order to classify what constitutes an "invasion of privacy," Warren and Brandeis created a six-part qualification scheme to attempt to balance the right to privacy of the individual against the right of the community to be informed. These stipulations include a narrower right to privacy for public figures; the right of an aggrieved party to respond; privacy protections for written or visual sources, but not oral sources; the abdication of privacy rights for information published by oneself; having truth be unimportant if privacy is violated; and lastly, the role of malicious intent in publishing damaging information. In each of these arguments, Warren and Brandeis justify the right to privacy relative to the existing social conditions and the rights of others to know information about us in select circumstances. Thus, their checks on privacy aim to make freedom of speech a relative right, and for privacy concerns to tip the scales away from disclosure of private facts.

The first of Warren and Brandeis' six stipulations argues for the weighing of privacy against the relative celebrity of the individual, and whether they have "renounced the right to live their lives screened from public observation"—for example, candidates for public office (Warren and Brandeis). Even then, privacy still does extend narrowly to people within the public eye; while public officials lose much of their right to privacy by virtue of existing and working in the public sphere, these officials are entitled to the privacy of past information, such that their entire pasts or intimate lives are not trawled

and laid bare for public inspection. Two, the right to privacy of an individual does not trump another's right to seek reparations for attacks on their character. Warren and Brandeis argue, an individual would be able to publish the vindicating parts of another's speech to clear their reputation and provide evidence for damages. Three, Warren and Brandeis discuss the difference between invasions of privacy in speech and in oral statements. Slander, or oral defamation, they assert, would not be granted the same protection as invasions of privacy in media or print sources. Since oral defamation or other gossip used to not persist through time or spread beyond a local area, they did not hold the same potential for personality damages or harms to reputation as print sources. Fourth, the right to privacy of an individual vanishes when an individual publishes information about themselves. Fifth, the truthfulness of a publication plays no role in the validity of its publication; the disclosure of true, private information (also called private facts) carries the same invasive harms that false speech does. Lastly, Warren and Brandeis argue that the absence of willful, malicious intent cannot serve as a defense for the media invading people's privacy. That is, the implied or expressed intent of a publisher to do no harm does not serve as a defense against emotional damage inflicted by privacy invasions. Thus, these six qualifications on the right to privacy were designed to combat flagrant violations of one's private life for the sake of a good story or salacious gossip, but to leave room for truthful facts to be disclosed in the public interest.

While the Warren and Brandeis tort envisions a solid foundational right to privacy in the common law framework of the United States, their privacy tort falls short when framed by current standards of media access and informational availability through the

internet. Warren and Brandeis opened up the discussion on the flexibility of the common law in new circumstances, yet even in recognizing the pace of change in a growing democracy, their envisioned right to privacy has not held up to evolving social conditions. Namely, the requirement that "oral publication" of material not be granted the same privacy protections as written publications reflects a much more insular society than we now know today. While Warren and Brandeis believed that in-person oral gossip would not spread beyond a small community, new technologies make possible the global dissemination of oral information. In the 1890's, Warren and Brandeis worried about the advent of the camera to capture revealing images of an individual's personal life, and in the 1960s, William Prosser objected to the oral publication of information in the age of radio, when radio "made written or printed information" obsolete (Prosser 1960, 394). And today, the risks of private information disclosures can occur through television, internet, and the myriad social media platforms that operate in the 21st century.

Secondly, the absence of privacy provided to information an individual discloses themselves reveals an unforeseen obstacle in the permanence of news and information today. Warren and Brandeis believed that information published by an individual could no longer be granted privacy protections; however, the reach and permanence of information in the digital age reflects how an individual can entirely lose control over everything from their own "likeness" to deeply personal information through the information circulating on the internet. Amy Gajda describes a relatable case where actor Hulk Hogan posted a photograph, only to later regret and delete it, but not before it made the rounds on Twitter. This looks towards the entire generation raised in the era of social

media dominance, who are all "publishers of Twitter, Instagram, Snapchat, and Facebook" with the potential to cause irreparable harm to themselves and other "internet bloggers" (Gajda 2015, 250). Given the ability for people to post potentially regrettable information with such permanent footprints, the loss of privacy rights to individuals upon publishing such information reflects a permanent relinquishing of control of one's own information that Warren and Brandeis could not have imagined.

Alternate Constructions of Tort Privacy

Although Warren and Brandeis created the initial outline for the right to privacy in the United States, much of their initial argument appeals to the moral side of personhood, rather than legal technicalities of inserting a right to privacy within the existing Constitutional framework. Their 'right to be let alone' entered into a decades-long battle with the courts that have continued to test the flexibility of common law and the power of judicial precedents around matters of privacy. However, since their argument in 1890, the harms caused by invasions of privacy remained largely beyond the purview of the Supreme Court and legislators, and any legal challenges upholding privacy have largely been unsuccessful.

Privacy and personality rights, in the Warren and Brandeis construction, did not have a clear enough attachment to existing Constitutional rights. In fact, since their tort, privacy protections have usually been denied across all levels of the court, where freedoms of the press have trumped an individual's privacy.

One tort, however, has been successfully integrated in a number of cases outlining the bounds of privacy. William Prosser, in an attempt to consolidate the right to privacy

imagined by Warren and Brandeis, wrote the 1960 “Privacy” tort, arguing that privacy is not one single tort, but rather a “complex of four” different rights to provide legal redress to individuals who have had their privacy violated. These four qualifiers of privacy are the intrusion into one’s personal life; public disclosure of embarrassing private facts (intrusion upon seclusion); publicity which misrepresents an individual (false light); and the appropriation of an individual’s name or likeness (Prosser 1960, 389). In each of these cases, Prosser argues, there is some grievous harm done to the individual, a harm that is deserving of emotional or mental damages recoverable under the law.

Prosser offers the following case in favor of the privacy protections for intrusions of privacy, even when the basic facts of the case are true. In the 1931 California court case of *Melvin v. Reid*, a woman had been a prostitute who was tried and acquitted for murder. Years later, the woman remarried, went by her married name of Melvin, and lived a peaceful life, where she purposefully distanced herself from her past. However, a movie called “The Red Kimono" exposed all of her past in this re-telling of the true events, causing an undue personality harm “by revealing her past to the world and her friends,” so she sued for an invasion of privacy (Ibid. 392). The California Appellate Court acknowledged the spotty record of the right to privacy in the courts, and that most successful cases rest on “breach of contract,” or that some fit neatly under the “law of libel without invoking the doctrine of the right of privacy” (Court of Appeals, Fourth District 112 Cal. App. 285, Cal. Ct. App. 1931). The court agreed that Melvin had suffered a grievous invasion and personality harm. Though the original common law did

not define a right to privacy, the court rested its decision on the violation of Melvin's right to pursue happiness, a right protected under the California Constitution.

This reflects similar logic regarding the right to privacy in the *Rachel* decision in France: a real photograph caused extreme emotional duress for a family, resulting in the need for an injunction of the image and financial reparations. The truth of the information played little role in the decision for the broad disclosure of her old life. Rather, the important legal opinions to come out of the *Melvin* decision in the California District Court were that *a)* Melvin had, in the years since the trial, made every effort to distance herself from her past life, and *b)* that the right of the public to know certain information is not absolute, and that the limits on the freedom of expression must at least consider the potential effects on a person's privacy.

In addition to Prosser's portrayal of the *Melvin* decision to exemplify how truth cannot be a defense to invasions of private facts, his treatise on privacy draws another limit on expectations of privacy: looking at the relative status of the individual making the claim to privacy. In particular, Prosser draws the reader's attention to people in the public eye. Prosser asserts that the press "has a privilege, guaranteed by the Constitution, to inform the public about those who have become legitimate matters of public interest," an interest that very often can oppose an individual's privacy (Ibid. 411). Given the potential "newsworthiness" of an individual's private life, Prosser doubles down on the idea that celebrities, public figures, and government officials—as well as "public figures for a season"— do not maintain the same basic rights to privacy as the common person, yet they still deserve of privacy in intimate moments with no relevance to their public

personality (Ibid. 413). Prosser tempers the right to privacy of the individual against the public's right to know.

While Prosser's main goal was to propose a classification scheme for privacy, and to provide order to roughly 80 years where privacy languished in an inhospitable court system, the end result has been that Prosser's envisioning of privacy as a multi-part civil protection has been neglected in post-1960 court decisions. Although privacy as a protection for personhood has become more firmly introduced into legal and social vernacular, the Supreme Court has largely rejected Prosser's construction of a distinct right to privacy in balancing the right to privacy with the public's right to know.

Evolving Standards of Newsworthiness

In a strict departure from Prosser's standards of privacy under the civil liability tort, court cases with connection to the media have been overwhelmingly decided in favor of the free press. Highlighting the power of First Amendment rights to freedom of the press in the United States, privacy of the individual holds little weight against the public interest, with one Oregon court stating that "a review of cases since 1967 had shown 'no reported case in which a plaintiff successfully recovered damages for truthful disclosure by the press'" (Gajda 2015, 45). The theoretical rights to privacy through tort law, envisioned first by Warren and Brandeis and later by Prosser, ran into the barrier of the First Amendment.

One case that demonstrates the strength of First Amendment claims is that of *New York Times v. Sullivan* (1964). The *New York Times* had run an ad soliciting donations for Martin Luther King Jr., who was being held in Alabama on perjury charges. L.B.

Sullivan, the city's Public Safety Commissioner, claimed that the ad misrepresented him and the Montgomery Police Department with factual inaccuracies, and he asked for a retraction of the ad. The Times refused, and Sullivan sued for libel, winning damages in a lower court. However, in a unanimous Supreme Court decision, the justices overturned the lower court's precedent in favor of the *Times* on First Amendment grounds, arguing that removing this ad would violate freedom of the press. Newspapers reliant on free speech worried that the ability to claim defamation, or any privacy protections, for public officials would suppress the watchdog functions of the media on government, and that it would provide public officials with an opportunity to legally fight criticism or allegations of abuses of power (Abrams 2021). In deciding the *Sullivan* case, the Supreme Court removed privacy protections and raised the bar considerably for successful defamation suits brought by people in the public eye. Thus, a new standard of defamation was developed in Justice Brennan's unanimously supported opinion, where individuals would have to prove "actual malice" of the publisher of defamatory information or libel, such that the publisher *intended* to cause emotional harm or otherwise damage an individual's reputation.

The decision in *Sullivan* reflects the attempts by the court to preserve freedom of expression for newsworthy information; however, it also reflects a massive obstacle to the principles of a right to privacy outside of a criminal context. In contrast to the decisions in support of a narrow right to privacy under the Fourth Amendment, defamation and civil liability for publishing information about another's personal life do not have the same considerations for privacy. The precedent set by *Sullivan* has led the

Supreme Court to apply these principles of a 'newsworthiness standard,' one that recognizes all manners of personal information as potentially important inclusions into the public record. That is, the "fear of a chilling effect" on a free media "has led the Court to protect even undesirable speech" (Zimmerman 1982, 383). This can be seen in the 1967 case of *Time v. Hill*, where James Hill and his family were denied damages in defamation suits because they could not prove that the publisher, *Life* magazine, had acted with "actual malice." This case created an expansion of the precedent in *Sullivan*; the higher threshold for public figures now applied to people tangentially in the public eye.

The Hill family were considered private individuals, until their unfortunate tragedy of being kidnapped at gunpoint had been elevated to "newsworthy" again through a play written about it; that is, they became public figures "for a season," to borrow from Prosser's language on temporary celebrity status (Prosser 1960, 413). In these instances defined by the Supreme Court, the information contains points of departure from the truth or otherwise misrepresents reality, yet the standard for people who have risen to the public eye in some form or another can lose all ability to seek damages. The 'relative public figure' status has been extended to almost all manners of defamation cases, from instances where news media publish the names of living rape victims, as in *Florida Star v. B.J.F.* (1989), or the sexuality of an active bystander who saved the life of a U.S. president, as in *Sipple v. Chronicle Publishing Co.* (1984). The standards for proving defamation are extraordinarily high, and "protection of rape victims, like protection of juvenile offenders, then, seemingly fail to reach that extraordinary threshold" that

governs the public disclosure of private facts (Gajda 2015, 35). That is, highly sensitive pieces of personal information can be aired in the public domain, regardless of damaging personal revelations.

However, these cases reflect a constant challenge in weighing the relevant "newsworthiness" of a story against the media's right to freedom of expression. As soon as a story becomes written and published, it becomes part of the public domain, and thus worthy of press coverage. In this circular logic, "whatever is in the news media is by definition newsworthy" and thus deserves First Amendment protections (Kalven 1967, 336). This trend towards total eclipses of the tort invasion of privacy predates *Sullivan*, and it can also be seen in *Sidis v. FR Pub. Corporation* (1938). Sidis was a prodigious child mathematician who achieved early celebrity status, yet whose subjection to the abuses of paparazzi and media invasion caused him to retreat entirely from the public eye, aiming to live a life of solitude. However, *The New Yorker* magazine published a story on child prodigies and their life trajectories, interviewing Sidis and others, subjecting him once again to the public consciousness. Sidis sued for libel and invasion of privacy against the magazine; however, he also claimed a "tort action for invasion of privacy by publication of embarrassing private facts," an argument built on the common law case precedents that existed in a handful of other states where the magazine had been sold (Barbas 2013, 34). Shutting down this argument for the invasions of privacy and the associated "emotional damages," the U.S. District Court of New York ruled that, by virtue of Sidis' youthful status as a celebrity, the magazine was free to publish all insights into his adult life. *The New Yorker*'s argument reflects similar circular logic, whereby an

individual featured in a story must thus be considered newsworthy. The *Sidis* case reflects how the scales are weighted towards expression, even to the extent of turning "personal humiliation into an object of mass consumption" (Barbas 2012, 26). In contrast to earlier state court decisions, the New York District Court came to an entirely different conclusion around the public interest than the California appeals court in *Melvin.* Melvin was able to seek emotional damages for the dredging up of her past life, whereas Sidis' past life as a celebrity became a justification for the continued invasion of privacy well into his new life of anonymity. This ultimately unsuccessful case demonstrates how the circular logic of "public interest" upholds the right to freedom of expression, ultimately resulting in the resounding defeat of civil claims upon a right to privacy.

Civil Liability versus Criminal Protections of Privacy

Although the Supreme Court has insisted on the public's right to know, the right to privacy has seen considerable protection in a criminal context, as a freedom from invasions of the government. In order to interrogate court challenges of privacy, the *Olmstead* case offers a glimpse into the challenge of adding privacy to the list of Constitutionally protected rights.

Three years before Prosser's exemplary privacy case of *Melvin v. Reid* reached the California appellate court as a "win" for privacy as a civil liability case, the Supreme Court heard the 1928 case *Olmstead v. United States*, where federal agents installed a wiretap into a person's home and office building in an effort to uncover criminal bootlegging. Olmstead argued that his Fourth Amendment rights against "unreasonable search and seizure" were violated with these wiretaps; even though the federal agents did

not physically invade his property in search of evidence. In a condemnation of the right to privacy, the Supreme Court asserted that the individual did not have Fourth Amendment protections to private phone calls, since there was no physical invasion of "property, personal effects, or papers" (Fourth Amendment). In the majority opinion, the facts of the case rested on whether the Fourth Amendment protects against invasions of privacy that do not cross a physical threshold, and the Court upheld that physical entry is required for invasions of privacy to occur.

While the *Olmstead* case rested on the Fourth Amendment right to privacy—as it pertained to unwarranted searches of *physical* property—both Warren and Brandeis' and Prosser's privacy torts embody the kind of connection to privacy as an intangible right deserving of protection, regardless of physical location. Prosser's key amendment to existing rules on privacy asked whether the invasion of privacy would be "offensive or objectionable to a reasonable man" (Prosser 1960, 391).

Whereas privacy was not recognized by the Supreme Court as a right of U.S. citizens until the mid-1960s, the new right to privacy in the United States reflects language that mirrors Prosser's understanding of privacy. In examining the right to privacy in the criminal context anew, the Supreme Court heard a challenge to the *Olmstead* precedent in the 1967 case *Katz v. United States*. Katz was taking a phone call in a public phone booth that federal agents had altered with a listening device. Phone calls that police had listened to were admitted as evidence of Katz's illegal activity, making *Katz* an almost-identical case to the *Olmstead* case. Drawing from the wealth of privacy scholarship in the preceding years, the Supreme Court reversed its original

decision in *Olmstead* to acknowledge that wiretapping did infringe upon an individual's reasonable expectation of privacy. In the majority opinion, Justice Potter Stewart wrote that the Fourth Amendment protects "people, not places," and asserted that the Fourth Amendment is actually a protection of privacy as it attaches to an individual.

Katz reflects an acknowledgment by the Supreme Court of an instance which demonstrates a partial ability for the common law to adapt in changing times and new technology. Thus, the cases which have successfully paved the way for privacy have been defined using criminal liability and the aftereffects of invasion of privacy. In contrast to the lofty language around "dignity and reputation" exhortations that emerge from Warren and Brandeis, the language used in *Katz* explicitly connects to existing rights in the Constitution in order to create a solid foundation for overturning the existing precedent in *Olmstead*, while also narrowing the legal definition of privacy. In addition to Justice Stewart's reinterpretation of existing precedent, Justice Harlan wrote an accompanying decision that echoes the standard of reasonableness. Harlan's accompanying decision created a "reasonableness" test for determining invasions of privacy under the Fourth Amendment, which exhibits concordance with Prosser's scholarship on invasions of privacy in the civil sphere. Justice Harlan's two-part test for whether an individual's Constitutionally guaranteed, albeit conditional, right to privacy has been infringed upon is a) whether an individual had an "actual, subjective expectation of privacy," and b) whether society at-large agrees and is "willing to recognize [that] as reasonable" (U.S. Reports, 389 U.S. 347, 361). Given these two factors, Harlan's qualification on a right to privacy protected by the Fourth Amendment does narrow an individual's right to privacy.

Conversations in public or things in plain view are not granted the same level of privacy protection as it would be for information that an individual has attempted to remove from public view.

This standard of reasonable expectations of privacy has continued today, extending privacy to the right of couples to use contraception (*Griswold v. Connecticut,* 1965) allowing abortions (*Roe v. Wade*, 1973), and prohibiting police from using thermal imaging technology without suitable requirements of a search (*Kyllo v. United States,* 2001). Indeed, these court decisions have reversed prior rulings that deny people the right to privacy within their homes and other private spaces.

Although the right to privacy in the courts has made leaps and bounds since the first theories of privacy, justices have largely refrained from creating law in the courts. Indeed, the way in which the courts have interpreted a right to privacy under the Fourth Amendment demonstrates justice's wariness to fully deliver any promise of widespread privacy, and to shy away from balancing between privacy and First Amendment rights to expression. This slow process of privacy within the U.S. common law can be seen with how the "reasonableness standard" has been applied in successive court cases to allow people to have privacy in their own homes, a lesser degree of privacy to vehicles, and privacy in communication to others through phones and letters. Each new development since *Katz* has required new court cases to develop the boundaries of the right to privacy under the Fourth Amendment. Even as the Supreme Court overturned previous decisions to guarantee an individual's privacy, the court also expressly denounced a comprehensive right to privacy, arguing that "the Fourth Amendment cannot be translated into a general

constitutional 'right to privacy.'" (389 U.S. 347, 350). Thus, each new Supreme Court precedent narrowly etches out potential expansions of 'reasonable' areas of privacy.

These court cases mark where the right to privacy became somewhat pigeonholed with the *Katz* decision. While the spirit of the law recognizes that the Fourth Amendment has some inherent characteristics of privacy ("being secure in one's *person* and effects," for example), the actual language of these monumental privacy decisions demonstrates not a commitment to privacy, rather a commitment to reigning in the powers of the government. In each Supreme Court case that supported the right to privacy—*Griswold, Katz,* and *Roe*—the right to privacy is constructed as protecting privacy rights against government intrusion; "the presence of government involvement in cases finding an invasion of privacy, however, is a glaring common denominator that supports the proposition that American privacy is understood as liberty from government" (Dowdell 2017, 330). Thus, because law enforcement plays an important role in the fundamental facts of each case, the protection of privacy must involve some attempt by the government to overreach a citizen's Constitutionally protected Fourth Amendment right.

The right to privacy has experienced a mixed record of success when defined in the civil, rather than criminal, context. In order to adapt to changing times, the Supreme Court has seemed more sympathetic to arguments about invasions of privacy from the government than invasions of privacy and damages of reputation by the press. However, Congress and individual states have also explored the right to privacy in statutes for approaching matters of protecting individual privacy in new informational realms.

Legislative Creations of Privacy

In addition to the convoluted case law on privacy—where the jurisprudence bifurcates into poorly-protected rights to privacy in terms of civil liability or tort law, and comparatively-better protected rights from the invasions by the government—the legislative construction of privacy reflects a similarly complex pathway. Rather than acknowledging a unified right to privacy, federal and state governments have pursued privacy in narrow circumstances, often only applying to specific industries or certain kinds of information deemed more “sensitive" than others. In particular, privacy has been upheld for financial, educational, and health records, while the opposite is true for digital privacy and online communications, as written in key federal statutes.

The origins of the legislative push for privacy began in 1973 with the Department of Health, Education, and Welfare (HEW), and is still being reworked today in 2022, with the development of state laws around digital privacy and consumer protections online. I will argue that the fragmented nature of the federal statutes around privacy do not adequately address issues of digital privacy, nor do they adequately represent the interests of people within the United States.

Beginning with the Department of Health, Education, and Welfare (HEW), the federal bureaucracy began to view the potential for digital information and the advent of new technologies to serve as both a boon to economic growth, as well as a risk for U.S. consumers in terms of data processing. In 1973, HEW released a 193-page report titled “Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems.” Among other topics, this report documented the various information that U.S. consumers may have to provide in these

new online spaces, from potentially identifying themselves through Social Security Numbers (SSNs) to the unnecessary storing of personal information about an individual. A main theme underscoring all of the report was the need to legislate in light of the rapid development of new technology relative to the slow formulation of law.

The law moving at a much slower pace than technology is one commonly discussed by cyber ethicists. As James Moor puts it, "computer sprawl moves on many fronts unsupervised, and the beginning of exponential growth in the field of computing has effects which none of us can imagine, let alone predict," meaning policy falls far behind the technological advancements (Moor 2000, 35). The HEW Report, then, aimed to fill this policy gap with concrete suggestions in order to allow for some semblance of laws and regulations to protect consumers. Explicitly underlining the unnavigated terrain of digital spaces, the HEW discussed how existing laws do not appropriately protect privacy: "The natural evolution of existing law will not protect personal privacy from the risks of computerized personal data systems" (HEW 1973, 47).

Addressing the potential risks for consumers' digital information, the HEW Report gave an overview of existing constructions of privacy in the United States, particularly the ways in which 'privacy' in the U.S. vernacular has fallen short. Alluding to existing jurisprudence from *Katz v. United States* on the reasonable expectations of privacy under the Fourth Amendment, the HEW Report highlights the challenges faced in reaching one single definition of privacy. Yet this bureaucratic agency, unlike Congress and the Supreme Court, did not shy away from offering a potential definition for privacy,

and one that recognizes the challenges of maintaining and balancing a right to privacy in digital spaces. It defined privacy as follows:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a *right to participate in deciding what the content of the record* will be, and what *disclosure and use will be made of the identifiable information in it*. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law. (1973 HEW Report pg. 49, *emphasis added*)

This rather liberal definition of privacy, relative to the narrowed understanding in the judicial branch, informed the HEW's recommendations to legislators to factor in consumer privacy and information-sharing in new legislation. The HEW Report demonstrated how privacy policy solutions would be shaped by the diagnoses of the risks to privacy, such that Congress must step in to legislate a pathway for digital privacy rights that aligns problems with solutions. Thus, based on its identification of the problems privacy would face in the digital age, the HEW developed a highly structured list of recommendations centered on a few main goals of protecting privacy online.

Among these key recommendations that the HEW delivered to legislators, the bureau argued for the creation of an independent federal agency to regulate "any automated personal data systems," which refers to any large bodies, governmental institutions, or private institutions which control considerable amounts of consumer data containing identifiable information (HEW 1973, 50). Additionally, they called for the creation of a five-part Code for "Fair Information Practice Principles" (FIPPs), which

allows individuals to a) know what kind of information exists online, b) safeguard the individual's information against improper/unfair uses, and c) to create actual enforcement mechanisms for invasions of privacy in digital spaces, which ranged from criminal to civil liability as well as injunctive relief for improper circulation of one's data, amongst other steps to ensure data privacy (Ibid. 55). Thus, the HEW Report encouraged government intervention into the realm of current technology and data use practices through the coordinated Fair Information Practices in order to protect citizens' information online.

While the intentions of the HEW Report were noble, the actual implementation of their recommendations fell largely on deaf ears. Although Congress soon passed the 1974 Privacy Act in the wake of the HEW Report's publication, the protections for consumers were limited to the potential abuses of an individual's privacy at the hands of the federal government. Influenced by government surveillance during the Watergate scandal, the 1974 Privacy Act implemented the HEW Report's original recommendations for FIPPs, including the safeguarding against abuses by governmental agencies surrounding personal information, and the rights of an individual to know and correct the type and extent of information held about them by agencies. Legal scholars and politicians both point to the adoption of the HEW Report's recommendations in a few key places, such that "Congress crafted a few industry-specific privacy statues, but left a large array of data collection and use unregulated" (Solove and Hartzog 2014, 593). Thus, the initial response to the 1973 HEW Report created the inklings of a right to privacy for U.S.

citizens in moving into online spaces, but the actual transition from recommendations into law failed to get off the ground.

The Privacy Act of 1974 responded to the growing social and governmental awareness about the risks of personal information online and the additional concerns brought up by the 1973 HEW Report. While the Privacy Act did establish some rights for U.S. citizens' data rights, the Act failed to incorporate the broader risks to individual privacy posed by tech corporations, larger businesses, and "Peeping Toms" in virtual spaces. However, another privacy statute, the Electronic Communications Privacy Act, developed over a decade later and extended more rights to private communication into the digital realm.

Interestingly, this successful privacy protection mirrors the rights of privacy defined by the Supreme Court when hearing cases around criminal liability and privacy from intrusions by the federal government. Indeed, the Electronic Communications Privacy Act (ECPA, 1986) established protections for "greater or lesser" invasions of privacy by other persons into an individual's life, from wiretapping phone calls to reading emails to poring over stored data. In this landmark legislation, individuals were granted statutory protection from invasions of privacy by others within phone calls, email and other digital communications (18 U.S. Code § 2511). Additionally, this statute defines the protocols required by federal agents in order to procure warrants for wiretapping and other digital surveillance, to ensure citizens retain Fourth Amendment rights against unreasonable searches and seizures. So, while exceptions are made to public officers or federal agencies (when appropriate warrants exist), the right to privacy established within

the ECPA attempts to serve as a check on unwieldy federal agencies while simultaneously extending greater protections into digital spaces for U.S. residents than previously existed.

In addition to the ECPA, four other privacy statutes emerged to allow some particularly vulnerable personal information to be protected through legislation. The Fair Credit Reporting Act (FRCA, 1970), the Family Educational Rights and Privacy Act (FERPA, 1973), the Health Insurance Portability and Accountability Act (HIPAA, 1996), and the Children's Online Privacy Protection Act (COPPA, 1998) all demonstrate the ways that the federal government has aimed to protect the privacy of U.S. citizens in narrow ways.

However, these privacy acts mainly serve to enforce some semblance of regulation around the potential risks for information. Yet, the obstacles to enforcement for digital privacy protections, as in the Children's Online Privacy Protection Act (COPPA), demonstrates how regulations online can often have easy workarounds, making them virtually unenforceable. For example, while COPPA protects children up to age 13 by requiring parental approval, websites and data controllers can circumvent this law by not asking for their users' age (Leta-Jones 2016, 67). Therefore, while these narrowed rights to privacy do serve an essential function in protecting personally identifiable information from prying eyes, they also do not form solid enough regulations to ensure enforceability of privacy rights, particularly online.

However, at the same time that privacy statutes were being added to the federal agenda, new legislation developments also sealed the fate for less-protected digital

privacy rights. For example, Section 230 of the Communications Decency Act (CDA, 1996) grants online service providers near-full immunity from rules around invasions of privacy online and publication of harmful information on their sites.

A Slow Rejection of the Right to Be Forgotten

Moving into the digital age, then, the right to digital privacy has faced a tough and inhospitable environment in the United States. The development of a unified right to privacy has failed to connect to existing civil rights within the Constitution and has limited enforceability in statutes, both of which have led to the outright rejection of widespread digital privacy for people in the United States. There is little legal baseline for privacy in the United States to develop in line with EU standards, let alone the standard of digital privacy as laid out by the GDPR. But the lack of digital privacy developments in the United States still bears examination. In this section, I will argue that the aforementioned fragmented approach to privacy, coupled with robust protections for the freedom of expression and for internet service providers (ISPs) and the exemption of data providers from Section 230 of the Communications Decency Act of 1996 (CDA), form obstacles to the development of an American right to be forgotten.

In addition to the fragmented constructions of privacy found in both the U.S. court system and in the legislature, other obstacles to a comprehensive right to digital privacy, such as the EU's right to be forgotten, come from one act of legislation in particular. The 1996 CDA originally had the very legitimate aim of "preventing any individuals from knowingly transmitting obscene content to minors," protecting U.S. children from being exposed to indecent communication and information online, in

addition to preventing consumers from being harassed over telecommunication lines (U.S. 47, Title V, Telecommunications Act).

However, this law also contained a seed of tech industry protections, whereby digital providers were given certain immunity from noticing, removing, or acknowledging unsavory or unsettling content on their services. Section 230 of the Communications Decency Act declared internet service providers and other data controllers exempt from the requirements of transmission of information: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S. Code § 230). This stipulation allows internet service providers to be free of liability for any information hosted on their sites. As Leta-Jones (2016) puts it, "Platforms and service providers are considered simply conduits for content," and U.S. law enforces no responsibility for solely allowing access to content (Leta-Jones 2016, 66). This key exemption for data service providers in the United States has created immense problems around data removal. In *Google Spain*, the defining link in digital privacy in the EU—of invoking the 1995 Data Protection Directive to request to remove information online—occurred because Google was classified as a "data controller." Meanwhile, in the United States, tech companies are designated "intermediaries," or entities that provide *access* to information, but hold no control over publishing information. While the Communications Decency Act was overturned in *Reno v. ACLU* (1997), where it was deemed to violate First Amendment rights to freedom of speech due to "overly broad" definitions of what constituted obscene material online, Section 230 has remained law, allowing publishing

sites and internet service providers to avoid liability for all manners of information posted on their sites.

Given these outsized protections for data processors, many third-party sites have been able to claim immunity from the law by not defining themselves as creators of information. Websites that host revenge porn and other "push-the-envelope" publications that circulate critical information about others are able to declare themselves immune since they define themselves as collectors and aggregators of information that solicit content from individuals (Gajda 2015, 123). Thus, Section 230 of the Communications Decency Act essentially holds no one accountable for the publication and continued circulation of emotionally damaging information online.

In the realm of the right to be forgotten, prime examples of information available for removal under the EU's GDPR rules include search engine results, such as articles to outdated news articles, or other notices that could appear online. However, under the immunity provided by Section 230, "the U.S. is incredibly unlikely to obstruct discoverability of personal information upon request," and any form of right to be forgotten-style measure of delisting information from search engines would be highly improbable under the existing regulatory conditions (Leta-Jones 2016, 151). Any digital privacy laws targeting search engines for cataloging truthful, but potentially reputationally-damaging information, must address how CDA 230 insulates the data providers that allow for uninhibited information circulation.

The theoretical limits of the right to digital privacy have been strained by the preexisting faults in conceptions of privacy, and unfavorable legislation like Section 230

has made it incredibly difficult to return power to consumers in the United States. However, mounting concerns over Big Tech's monopoly on private citizen's data have resulted in increased legislative, executive, and bureaucratic pressure to develop comprehensive digital privacy rights for people in the United States.

Section 230 reflects the tipping of the pendulum towards internet service providers, away from consumer protections. Before Section 230, rulings like those in New York District Court's *Cubby, Inc. v. CompuServe Inc*. (1991) and *Stratton Oakmont v. Prodigy* (1995) demonstrated that internet providers were punished when they attempted to moderate online spaces; Prodigy faced liability for attempting to moderate their website, while Compuserve was treated as a content library. Evidence of moderation—filtering of people's online discourse of posts online—became evidence of liability for not catching every type of harmful content that went unnoticed by the content moderators. However, the underlying assumption for Section 230 is that the legal distinction between publishers and distributors of online information has become "a proxy for conversation about the First Amendment," (Stepanyuk 2022). That is, First Amendment concerns around freedom of speech have not really been explored within the internet environment, because Section 230 allows selective moderation by service providers with no agreed-upon framework for moderation. Indeed, the precedent-setting case of *Zeran v. America Online (AOL)* (1997) underscores this continued immunity, where the Virginia District Court upheld that search engines were immune from tort liability for posts and publications on their services. In the decision, the judges decided that preserving the free market of the internet was more important than individual

intrusions upon privacy, and Section 230 allows internet providers to avoid "the specter of tort liability in an area of such prolific speech [the Internet] and the chilling effect" of allowing checks on internet providers (Ziniti 2008, 587). Thus, the capitalist forces of the internet and the power of Section 230 have led to the continued shutdown of civil liability torts, defamation, and any other privacy-based litigation to fail due to the prospect for growth of the internet.

Yet, even with an apparent preference for the free market of the internet, online privacy has been explored within the U.S. bureaucracy, Congress, and other governmental actors. From the HEW Report, which first described the unregulated internet as a potential risk to U.S. citizens, to the 2012 Internet Policy Task Force under the Federal Communications Commission (FCC), the U.S. government has expressed numerous concerns about the fate of consumer privacy in digital spaces.

In this 2012 Report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," the FCC released recommendations to Congress about expanding digital privacy and consumer digital protection frameworks, in order to ensure equitable interactions on the internet, and that U.S. consumers retain civil liberties online. The largest takeaways from this report were a) the recommendation for a "Consumer Privacy Bill of Rights," and b) to meet a standard of "global interoperability" to allow for reducing transaction costs between countries, and to provide for more uniform, agile protections of online spaces as new technologies continue to develop (2012 FCC Report, 35-37). This report identified digital protections as an important new avenue of policy

directions for the United States, not only to align with developing global standards of privacy online, but to provide actual enforcement mechanisms to errant tech companies, and to hold technology corporations responsible for violations of privacy online.

One of the main selling points of this report was the appeal to relevant stakeholders. In addition to pushing the legislative agenda for the Consumer Privacy Bill of Rights, the FCC also appealed to all varieties of corporate and advocacy groups who would like to join in the process of "deliberating and adopting" the new codes of conduct for privacy online (Ibid. 26). In contrast to the more adversarial approach to technology corporations by the European Union's GDPR, the U.S. government sees internet service providers and tech companies as potential allies, and that protecting digital privacy online is a point of common interest between the corporate interests and governmental regulatory players.

The main innovation in this report is the suggestion that Congress create a statutory Consumer Privacy Bill of Rights, based on the "Fair Information Practice Principles" (FIPPs), which were developed by the Department of Health, Education, and Welfare in its initial 1973 report. These statutory rights include the rights to individual control about how companies are using data; transparency about use practices; respect for the context that a consumer originally shared the data; security; time-limited collection; and holding technology providers accountable for violating consumer rights (Ibid. 11-22). The Consumer Privacy Bill of Rights aimed to use statutory avenues to fill gaps in consumers' right to privacy, and to use the might of the Federal Trade Commission

(FTC) to encourage technology companies to participate in their own regulation in order to extend some protections to U.S. consumers online.

While the report does lay out important steps to encourage self-regulation and participation by internet service providers in the regulatory agenda, the FCC's recommendations also encourage internet consumers to practice mindful sharing of information online. In acknowledging the risks and potential digital life cycle of information that consumers can give out, the report also advises that "consumers take responsibility for those decisions" about whether to post and circulate information (FCC Report 2012, 13). Reflecting a similar outlook to the sharing of personal information as that of Warren and Brandeis, the FCC's report expresses that an individual who shares information about themselves will lose the right to privacy and control over that information, so the initial act of sharing information is a first-order control on information privacy; an individual then bears responsibility for risks in online spaces and for ensuring their own digital privacy.

With a renewed push for citizens' privacy—data privacy in particular—the Obama Administration's FTC appeared to make digital privacy a priority in his second term. Indeed, their reasoning for becoming enforcers of consumer privacy online embraces a broad definition of privacy as both a tangible and intangible right, that "privacy protects important personal interests. Not just freedom from identity theft, financial loss, or other economic harms but also from concerns that intimate, personal details could become grist for the mills of public embarrassment" (2016 Federal Register). Solove and Hartzog argue that, due to these regulatory measures, "FTC privacy

jurisprudence is the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort" (Solove and Hartzog 2014, 587). However, the legal push behind a right to privacy has not been aligned with the policy recommendations of the FTC and the White House. A version of the Consumer Privacy Protection Act was introduced in the Senate in 2015, and again in 2019 with the Privacy Bill of Rights Act—both of which would have mandated that all internet service providers abide by the Consumer Privacy Bill of Rights and pre-existing FIPPs (S.1158 & S. 1214). However, this bill failed to go further than the Senate Judiciary Committee, and Congress has yet to hear other developments on the federal statutory level for consumer protections online.

Thus, internet privacy in the United States has largely been curbed in moving from policy recommendations into statutory rights or other protections under law. Following a similar trajectory to the right to privacy in the judicial system, the right to digital privacy in the legislature faces steep barriers from existing laws around immunity for service providers, and the inability, thus far, to translate regulatory interests into law.

Criminal Justice and the Impossibility of Forgetting

While the right to be forgotten could have monumental effects for the digital privacy of everyday individuals, the potential benefits of digital privacy could be particularly useful to people in the United States with histories of criminal records. Lageson (2016, 2020) discusses how the collateral consequences from having an arrest record, a criminal record, or any history of criminal sanctions can result in profound political, social, and economic consequences for people in the United States. Moving into

the digital age, then, the online re-publication of records can be extremely damaging, and can add insult to injury for people hoping to move beyond their past actions. Allowing the default of remembering an individual's missteps, in effect, fixes behavior and prevents any form of forgiveness.

In the United States, nearly one-third of adult Americans have some form of criminal record (Friedman 2015). Although having a criminal record has become increasingly common with aggressive sentencing and new crime bills, the costs and consequences faced by people with criminal records have also become more common. However, in recognizing the barriers to reintegration (and the positive outcomes that can be generated from encouraging ex-offenders to reintegrate into society) we must acknowledge how internet records and an absence of digital privacy have dealt major blows to forgiving ex-offenders.

Under federal laws, Congress has left the majority of record enforcement and the punishment of criminals, as well as rules around record expungement, to the state. Expungement—or the legal process of removing, sealing, or destroying an individual's criminal record—allows individuals to move beyond their actions of wrongdoing and pursue more meaningful reintegration into society. Indeed, it can "soften the severity of post-incarceration consequences" by removing public knowledge of one's wrongdoing, and it can aid in applying for jobs and finding housing (Silva 2011, 158). However, the process of seeking expungements can be costly for individuals to pursue, and records available for expungement vary by state, which highlights its mixed success. While the usefulness of expungement policies varies by state, 45 out of 50 U.S. states offer some

judicial or legislative process for removing information off of one's record. Usually, an individual must wait for a certain period of time after their sentence to show that they have attempted to grow from their acts of wrongdoing. This period ranges in time, and the crimes eligible for expungement range from only arrest records (non-conviction) to single felonies, misdemeanors, or in the most restrictive states, relief only for groups specifically "deserving of leniency," such as juvenile offenders or people who are victims of trafficking (Colgate Love 2022, 52-56). Likewise, in the most grave instances of violence, such as murder, sexual offenses, or crimes against children, criminal record expungement is impossible at the felony level, and only occasionally successful with misdemeanor offenses.

Although expungement practices do offer some lessening of the harsh collateral consequences faced by former offenders, they are also heavily criticized for failing to situate rehabilitation in a community approach. Recognizing the community's role in encouraging prosocial behavior—rather than as an engine of perpetuating punishment through stigma and social isolation—is one that the U.S. does not take kindly to. Rather, expungement is considered a deeply flawed practice for providing rehabilitation options to previous offenders, in that it fails to reckon with the broader societal conditions that so deeply stigmatize having a criminal record (Colgate Love 2003, Lageson 2022). While it is an imperfect tool for allowing individuals to move beyond their records, expungement has provided amelioration of the harsh collateral consequences faced by many individuals. Community stigma for people with records of incarceration not only reflects

an additional barrier to their reintegration into society, but an immovable obstacle to moving on in the era of the internet.

The case of *Martin v. Hearst* (2015) demonstrates how expungement statutes have struggled to maintain usefulness in the digital age. Lorraine Martin and her two sons were arrested on drug possession charges. Many news outlets owned by Hearst Publishing Co. reported on this case, posting the articles online. The charges were eventually dropped by the state, and Martin had her arrest record erased under the Connecticut Statute Record Erasure, then sought to have the newspapers remove the information in kind. However, when the newspaper refused, Martin sued the newspaper corporation for libelous depiction of her under false light and negligent infliction of emotional distress. However, the Second District Court of appeals decided in favor of the newspaper. In the case, the criminal expungements were found to represent the "legal truth," that in the eyes of the state government, Martin had not been arrested; while the media organization could likewise not be sued for false light claims, since Martin's arrest was factually accurate (Leta-Jones 2016, 65). This case highlights how, even after expungement, an individual cannot escape the history of their criminal records due to its ready availability online.

Moving into the digital age, the ability for individuals to seek relief through the expungement process reflects a fundamental flaw of expecting privacy and secrecy in a process that has developed concurrently with rapid, easy dissemination of any and all types of criminal records. Violations of privacy, and of the underlying tenets geared towards forgiveness, include numerous sources that publish information relating to individuals' criminal and arrest records. These include "public and private databases,"

from third-party mugshot websites that publish booking photos of individuals (regardless of conviction or charging status) to newspaper articles which dredge up decades-old convictions after individuals have attempted to move on (Lageson 2016, 138). Expungement statutes, which intend to prevent (to some degree) the community from knowing about individuals when they have made attempts to amend, do not protect the at-will harvesting of information at a price.

Thus, criminal justice reforms in the United States have suffered implementation issues at the hands of the internet. 'Clean slate' mechanisms fail to deliver real forgetfulness to people seeking forgiveness of their crimes. That is, expungement does not provide any opportunity for forgetfulness of one's past actions, even though the purported goal of expungement is one that allows forgiveness of one's past. From third-party databases that amass and reproduce mugshots and criminal records, to news articles on the internet that prevent an individual from receiving the benefits of erasure of records, many clean slate initiatives aim to allow for reintegration of individuals with histories of incarceration. However, without an active ability to remove associated stories and information relating to arrests and convictions, criminal expungement pathways are largely non- fungible in the technological age.

Section V: Policy Directions for the Digital Privacy in the United States

Throughout the history of the United States, privacy has been a muddled topic. Legal theorists have tried to define privacy as a civil liability tort, where invasions of privacy amount to damage to an individual's inviolable personality rights. In these attempts to chart a path for a right to privacy to be integrated into existing civil liberties,

the common law system was thought to be a boon to precipitate personality rights within the Constitution. However, the right to privacy has languished in the judicial branch, due to the Supreme Court's refusal to compromise any grounds of freedom of expression. Instead, courts have bifurcated privacy into a right to be free from government intrusion under the Fourth Amendment, and a rarer right to privacy in cases involving invasions of privacy and a 'reasonable person' standard.

In contrast, legislative decisions have tended to support access to the free market and competition online, rather than consumer privacy. Laws like Section 230 allow internet service providers to avoid responsibility for information posted on their servers, even for potentially libelous or privacy-invading information about others online (Gajda 2015, 125). Similarly, the statutory evolution of a right to privacy has been narrowly focused, with Congress declaring privacy to be available only for sensitive information (such as health records, education, children's digital privacy, and information held by federal agencies).

This lack of legislation in the U.S. also reflects a larger trend to "look more readily" to markets in order to solve problems facing consumers (Leta-Jones 2016, 74); that is, including corporations in proposed digital privacy solutions, and allowing market pressures to dictate the options of privacy available to consumers. When consumers 'demand' privacy, the U.S.'s capitalist expectation is that some online provider will likely 'supply' ways of integrating privacy into an individual's online experience. However, this use of the market to regulate what many, including EU lawmakers, believe to be a fundamental human right of privacy, reflects a failure of the right in that it is only

available to the privileged "Americans with means" who can afford to use for-profit websites that help to clean up people's reputation online (Ibid. 74).

While serious obstacles still exist for comprehensive digital privacy regulations, many are hopeful that the changing frontiers of privacy will, by necessity, be reconsidered in light of the rapidly evolving internet. In this section, I will discuss some of the policy directions that have been proposed for digital privacy for U.S. consumers, some which align more neatly with the GDPR's 'right to be forgotten' than others. I will mostly focus on proposed initiatives around amending or repealing Section 230, engaging in some degree of federal legislation of a right to privacy, the many state developments of consumer digital protections, and lastly, the possibility for re-evaluation of the right to privacy in the judicial branch.

Jeffrey Rosen argues that a requirement by Google to delist links about individuals would transform Google from a neutral arbiter into a "censor-in-chief," rather than a "neutral" force (Rosen 2012). However, Rosen's key presumption that Google and other search engines were ever neutral speaks to the challenges of writing code and algorithms. Yet, this assumption is wrong: "data are not neutral" (Kim 2017; p. 860). Written by humans, the code Google uses already does remove or filter content that it believes could be offensive to users or other violations of the community guidelines of the website. The market forces already "enable nontransparent filtering" beyond the overly broad standard that repealed the Communications Decency Act in the first place (Lessig 2008, 257). Filtering and deciding what gets to go online demonstrates that Google and other search engines already participate in the censorship and moderation of

content; there is just no body of oversight, and the internet search providers entirely escape liability for what they choose to remove or not.

Thus, efforts have been made in recent years to attempt some broad internet reforms through legislation. Republicans in Congress, such as Lindsey Graham (R-SC) and Josh Hawley (R-MO), have advocated for either large-scale reforms or complete repeal to Section 230 in order to stop "politically-minded censorship" of search engines and social media networks (Robertson 2019). Indeed, there has been a marked political bent in discussions over the past election cycle about Section 230; many Democrats argue that internet providers must accept more of a role in moderating content on their sites, such as claims of fake news emerging on Facebook, while Republicans argue that internet providers and social networks moderate excessively, engaging in political censorship of Republicans, as with the removal of Donald Trump from most major social media sites (Ibid.). Thus, with potential for bipartisan support, Section 230 could see some amendments or a process of repealing and replacing the law with one that forces search engines to be more responsible for the information they host online.

However, calls to repeal Section 230 are met with staunch opposition from the tech community, and from legal scholars, some of whom object to the existing immunity of tech companies under Section 230. Ziniti (2008) argues that the immunity ISPs have under Section 230 is a necessary part of the "long tail of Web 2.0" (Ziniti 2008, p. 593). In this environment, digital citizens are able to harness the growth of the internet with open-source software, new and better code, and the internet is able to deliver on the highly "generative" environment of the internet without the government infringing on the

growing value of the internet (Zittrain 2008, 65). In this view, over time, with more data and a sensitivity by tech corporations towards privacy rights, the internet and ISPs will self-correct, 'fixing the bugs' of past versions of the Web.

Weighing the freedom of the current internet versus the 'chilling effect' of potential digital regulations, I think there are merits to both arguments. A chilling effect on the developments of the internet would not reflect well on the free-market capitalist approach that the United States has historically taken to regulating big business and growing industries. However, the binary that Section 230 established, between either full liability or full immunity for ISPs, sets up an impossible choice that obfuscates real issues of invasions of privacy faced by U.S. digital consumers. Although Section 230 has its detriments, a repeal of Section 230 and the sudden presence of immunity for internet content would likely result in a chilling effect on new development on the internet and would probably be overturned by the Supreme Court (Ziniti 2008, 595 & 607). Thus, I would argue for amending Section 230 to strike a medium ground. Short of full immunity for technology companies, numerous additions to the law could further protect consumers online and draw technology companies towards brainstorming and creating new manners of 'generative activity' to occur on the internet. I imagine that something along the lines of Frank Pasquale's "right to respond," where search engines link an asterisk to allow for responses by individuals to unfavorable articles, could serve as a partial solution to allow for people to at least reckon with information posted about them online (Pasquale 2015, 523). Similar algorithmic fixes have been proposed by Lawrence Lessig and Viktor Mayer-Schönberger. Mayer-Schönberger has proposed metadata expiration dates for

most links, which would prevent the casual peruser of the internet from inadvertently stumbling on the embarrassing past mistakes of another person, while also not being a total barrier to invested parties finding the information (Mayor-Scönberger 2009, 179). Likewise, Lessig suggests that "architecture" and the ways in which companies develop code can be regulated by fixed constraints that can apply evenly across the internet (Lessig 2008, 345).

Thus, while Section 230 is far from perfect, a vacuum of guidance for internet companies would not stand in the current court system. That being said, the risks to individuals from invasions of privacy online are so great that the balance must not automatically tip towards big technology companies.

In addition to current agitations around Section 230, there have also been bipartisan proposals in Congress to use antitrust practices to regulate U.S. citizens' privacy online. Senators Amy Klobuchar (D-MN) and Marsha Blackburn (R-TN) have proposed an antitrust amendment to protect privacy, to weaken internet search providers' monopolies over consumer data. The ability for Google and large technology companies to amass large amounts of personal data demonstrates a different risk to privacy, that individuals do not know what information different web browsers are collecting from consumers. Given the 76 workdays per year that it would take for the average person to read every privacy policy they encounter, the amount of information we blindly cede to search providers reflects a lack of digital literacy by consumers unaware of the data privacy costs of interacting online (Leta-Jones 2016, 86). Discussing the monopolistic advantage that Google in particular has over other search engines, Pasquale describes it

as “self-reinforcing; the better it is, the more searchers use it, and the more searchers use it, the more data it has for improving itself” (Pasquale 2015, 527). Consumers are giving data away in unknowable ways, and this data allows for the consolidation of a handful of the largest internet corporations. However, with the General Data Protection Regulation to combat corporate threats to consumer digital privacy in the EU, European proponents argue that using antitrust law to protect privacy online is something that the GDPR and the State Data Protection Authorities (DPAs) can already do much better and with legitimate authority (Meyer 2019). However, given this potential workaround for digital privacy in the United States, an antitrust law could help weaken Big Technology’s chokehold and allow for the reinforcement of digital privacy into U.S. legislation.

In addition to these federal proposals for expanding digital privacy rights of U.S. technology users, many states have begun to champion a state-level right to privacy. With California, Colorado, and Virginia leading the charge, these states have adopted legislation around consumer privacy protections. For example, California has pushed the U.S. conception of privacy through the passage of many digital privacy laws, with the first around the digital privacy of minors in 2013 under the Privacy Rights for California Minors in the Digital World. This law allowed Californians under the age of 18 to remove information that they themselves had posted online. While republished versions were not removed, this law did become one of the “few circumstances under U.S. law that allows truthful information to be retracted from the public domain,” second only to copyright laws (Leta-Jones 2016, 68). This heightened regulation of digital

privacy for children also paved the way for further privacy developments for all California consumers online.

Next, with the California Consumer Privacy Act of 2018 (CCPA) and California Consumer Privacy Rights Act (CPRA) in 2018 and 2020, respectively. The CCPA allows for individuals to opt-out of data collection practices, allows individuals to request the information that any business holds on them, and perhaps most importantly, allows consumers to request that the business delete the personal information (California Civil Code, 1798.105 a). Under Proposition 24, the California Consumer Privacy Rights Act (CPRA) established a further-reaching digital privacy protection for California digital consumers, one that mirrors the language of the EU's GDPR. Backing up the 'right to delete' present in the CCPA, the CPRA maintains that an individual can request the right to delete any information held by a business. Additionally, the CPRA established a California Consumer Protection Agency to handle appeals and enforcement of the right to delete statute. Combining statutory language of the rights of the California consumer, which situates the right to digital privacy within fundamental rights of the person, allows for increased enforceability of these state-level policy implementations.

Likewise, a 2021 statute granted the right to digital privacy to Colorado internet users. Under the Colorado Consumer Protection Act, Coloradans have the right to "access, correct, or delete personal data, and the right to opt-out of the sale of personal data," granting the Office of the Attorney General the right to enforce and impose sanctions on "controllers" who violate this law (2021 S.B. 190, 6-1-1302). Lastly, in Virginia, the 2021 Consumer Data Protection Act (CDPA) also applies to large data

controllers (businesses which have access to the data of 100,000 consumers or more), and it outlines the rights to privacy of the citizen to "access, correct, or delete" data, as well as to empower the Attorney General and the Consumer Privacy Fund to enforce the law.

In all three of these states, the language around the right to digital privacy mirrors the language of the GDPR, albeit using "consumer" instead of "data subject," and "delete" instead of "erase." However, the implications around these laws are that the states, tired of the slow developments of the right to digital privacy at the federal level, have proposed digital privacy rights within their states. Likewise, similar digital privacy bills have been proposed to the State legislatures in Utah, Iowa, Minnesota, Massachusetts, New York, and a handful of other states (IAPP US State Privacy Legislation Tracker).

The success of these policies has not been measured yet, but in theory, these state provisions will certainly raise the costs of operating for internet service providers within their state. In general, this may signal that the 'will of the people' is changing towards wanting the government to step in to legislate privacy rights. Yet, in responding to individual state's rules about digital privacy, the rise in transactional costs shouldered both by state regulators and by technology corporations could foreshadow the adoption of a federal right to privacy.

While these many regulatory and statutory proposals for a right to digital privacy in the United States appear promising, the issue of First Amendment rights still hangs over the Constitutionality of these laws. In passing laws about the "deletion" of material online, strong proponents of the First Amendment will likely be the first to raise the cry

of censorship. However, given the changing conditions of the technological landscape, the changing preferences of U.S. citizens towards some nuanced balancing of a right to privacy, the Supreme Court may eventually be called upon again to hear the issue of privacy online. With the ability to overturn long standing precedent, the Supreme Court has reinterpreted the Constitution in deference to the changing mores and cultural norms of society. From *Olmstead* to *Katz*, the Supreme Court changed its tune around what constituted an invasion of privacy, considering changing public opinion and the ubiquity of new technologies.

This approach of judicial activism, in light of information that the Founding Fathers could never have imagined, does potentially hold promise in the long-term for navigating the right to digital privacy for U.S. consumers. In looking at digital privacy laws developed at the turn of the 21st Century, some scholars observed that Congressional movement to legislate online was actually slowing down judicial developments, and that "statutory changes cut short the natural adaptation of the law to the internet" (Ziniti 2008, 596-597). Thus, some have faith that, although the common law may take longer to come around, situating rights to privacy within Constitutional parameters reflects a cementation of privacy rights as a fundamental value of the American public, and one that deserves protection under the Constitution. Perhaps digital privacy, and the right to be forgotten, will once again force the U.S. courts to reconsider the Constitutional protections granted to the citizen.

Conclusion

In this paper, I have aimed to provide an overview of the historical and legal conditions that led to a right to be forgotten in the EU. In looking at France as a model country for digital privacy, France's existing traditions of upholding privacy as a "personality" right have made the transition into virtual space a small jump of technological implementation and holding search engines accountable for the information that they show to internet users. The right to privacy as a reputational concern has allowed the French GDPR Law to expand the principles within the EU-wide General Data Protection Regulation and introduce a distinctly French approach to the right to be forgotten online.

In contrast, the unsteady legal ground of privacy in the United States has made a right to privacy (thus far) all but impossible within the confines of the common law legal system and in the shadow of the First Amendment. Indeed, a constitutional right to privacy has been narrowly defined under the Fourth Amendment to mean freedom from governmental intrusion, while other privacy rights—such as the right to be free of invasions of privacy from fellow citizens or the media—have fallen to the wayside in U.S. jurisprudence.

Still, growing concerns over the risks to individual privacy has led to a marked increase in the statutory and regulatory arenas. In 1973, a report on the "Records, Computers, and the Rights of Citizens" developed most of the standards around fair information practices and principles (FIPPs) and data use practices, which have been adopted and implemented globally, including the digital privacy rights outlined by the General Data Protection Regulation in 2018.

Applying the lessons of data protection to criminal justice spheres, I expected to find that countries with fewer privacy protections for ex-offenders would burden individuals with the baggage of past wrongdoing. If that relationship was not so clear in the distant past, I find that digitization has exposed this latent problem: there appears now to be a large reciprocal relationship between rehabilitation as a criminal justice practice and digital privacy as a mechanism to pursue reintegration.

These cases offer contrast to this broad portrait of privacy as a necessity of criminal justice reform. In France, the goals of reintegration are second only to strong rights to privacy for all, with privacy rights providing additional reintegration help to former offenders. France's criminal justice structures allow individuals to move past their acts of transgression, and the government aims to encourage prosocial behavior in order to help former offenders reintegrate into society and desist from crime. The opposite pattern emerges in the United States. A slow, multivalent construction of privacy in both civil and criminal cases has left little room for obscurity around an individual's right to conceal information about themselves. The United States has implicitly continued this transparency into criminal justice spheres. With an immediately available database of criminal records online, an individual's ability to move beyond one's past actions becomes near-impossible with the perpetuity of online documentation, with First Amendment claims bolstering online providers to be able to show any personal information online.

This thesis attempts to reconcile understandings of forgiveness in the criminal justice sense with practical mechanisms of forgetting online. The dyadic relationship

between forgiveness and forgetfulness reflects how each process complements the other. Forgiveness requires an honest appraisal of the harms done to society from one's transgressions, but it also provides a restorative justice approach to harms caused within the community. Forgetting, meanwhile, holds the intentional obscurity of information as a goal in itself; that we are all entitled to 'clean slates' to the actions of our past, whether criminal or not. If complete information is entirely available to society, an individual cannot move forward from their past and regain standing within their community. Stigma and irrevocable online information both form intense social barriers to rehabilitation with no path forward for ex-offenders. Conversely, forgetting without forgiving removes the certification of an individual's restoration, and does not honor the growth that must necessarily be a part of the reintegration process. We must recognize the harms caused by transgressing social norms and laws, while also acknowledging that community forgiveness cannot be leveraged for perpetuity around one's past.

The right to be forgotten challenges conventional wisdom around what it means to remember, and challenges us as citizens interacting with the digital world, to ask ourselves whether remembrance is a noble pursuit. The right to be forgotten relies on a community pact, that I will not pry into your past if you extend me the same courtesy. The right to digital privacy, then, must reframe privacy as a social good, or that which is beneficial to me and my neighbor. It is this idea of "privacy as a social good" that reflects the value in preserving spaces of autonomy and obscurity; removing widespread community knowledge of our missteps means that we can reinvent and transform beyond the worst parts of our past (Regan 2011; 498). Privacy, and the ability to exist without

unwanted social intrusions, is a foundational component of participation in society. Under this frame of thought, privacy must be valued by the community, and strong protections must be built into law and social norms in order for renewal to occur.

Thus, in order to actually reckon with the right to privacy in the United States, we will likely have to question the assumption of First Amendment supremacy, and to place privacy in a larger social context. However likely it is that Americans would enjoy the right to be forgotten, this would require a radical shift in policy, social norms, and algorithms from remembering to intentionally forgetting in order to allow citizens of the internet to distance themselves from their pasts and reconcile with society. Short of radical, cultural change, this relationship between forgiveness and forgetting reflects how criminal justice reform almost demands a systematic approach to absolution of one's wrongdoings, and digital privacy concerns have forced us to reckon with our personal data habits and information we post online. Perhaps the right to be forgotten will put digital privacy into language that allows for inspection of how we legislate matters of wrongdoing, and will allow policy to deliver on the social and legal promises of forgiveness.

References

Abrams, Floyd. October 22, 2021. “The Supreme Court Faces a Huge Test on Libel Law.” *The New York Times.*

Alschuler, Albert. (2003). “The changing purpose of criminal punishment: a retrospective on the past century and some thoughts about the next.” *Chicago Law Review.* Vol. 6, Winter.

Audit, Bernard. (1977). “Recent revisions of the French civil code.” *La. L. Rev*., 38, 747.

Auxier, Brooke. (January 27, 2020). “Most Americans support the right to have some personal info removed from online searches.” *Pew Research Center.*

Barbas, Samantha. 2012. “The Sidis Case and the Origins of Modern Privacy Law.” *Columbia Journal of Law and the Arts.* SUNY Buffalo Law and The Baldy Center for Law and Social Policy.

Bennett, C. J. (2011). “In defense of privacy: the concept and the regime.” *Surveillance & Society*. 8(4), 485-496.

Beverley-Smith, H., Ohly, A., & Lucas-Schloetter, A. (2005). “French law. In Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation.” *Cambridge Intellectual Property and Information Law*, pp. 147-205.

Bode, Leticia and Meg Leta-Jones. 2018. “Do Americans Want a Right to be Forgotten? Estimating Public Support for Digital Erasure Legislation.” *Policy and Internet.* DOI: *10.1002/poi3.174*

Borgesius, Frederik Zuiderveen. 2018. “Privacy, Freedom of Expression, and the Right to be Forgotten.” *Cambridge Handbook of Consumer Privacy.*

Brimblecombe, F., & Phillipson, G. (2018). Regaining Digital Privacy: The New Right to Be Forgotten and Online Expression. Canadian Journal of Comparative and Contemporary Law, 4, 1-66.

Brock, George. 2016. *The Right to Be Forgotten: Privacy and Media in the Digital Age.* Bloomsbury Publishing.

Brunette, Robert. 1972. “Rehabilitation, Privacy and Freedom of the Press—Striking a New Balance: *Briscoe v. Reader's Digest Association.*” *5 Loy. L.A. L. Rev*. 544.

Californians for Safety and Justice. 2018. “Repairing the Road to Redemption in California.” *Second Chance Project Annual Report.* https://safeandjust.org/wp-content/uploads/CSJ_SecondChances-ONLINE-May14.pdf

Cheh, Mary M. (1991). “Constitutional limits on using civil remedies to achieve criminal law objectives: understanding and transcending the criminal-civil law distinction.” *Hastings Law Journal*, 42(5), 1325-1414.

Chin, Gabriel. 2016. August 2012. “The New Civil Death: Rethinking Punishment in the Era of Mass Conviction.” *UC Davis Legal Studies Research Paper Series. Research Paper 302.*

Clean Slate Initiative. “Clean Slate Initiative Celebrates Passage of Michigan’s Automated Criminal Record Expungement Legislation.” Website.

Commerce Department’s Internet Policy Task Force. 2010. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” White House, Obama Administration Report.

Council of Europe. 1981. “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.” *Strasbourg 28/01/1981 - Treaty open for signature by the member States and for accession by non-member States.* ETS-Treaty 108.

Craven, J. B. (1976). Personhood: The Right to Be Let Alone. *Duke Law Journal*, 1976(4), 699–720.

DATA\, P. O. P. (1995). “Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” *Official Journal L*, 281(23/11), 0031-0050.

De Baets, Antoon. (2016). A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology,* 30:1-2, 57-66.

Department of Health, Education, and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems. June 25, 1973. “Records, Computers, and the Rights of Citizens.” *HEW Report*.

Deringer, Kathryn. (2003) "Privacy and the Press: The Convergence of British and French Law in Accordance with the European Convention of Human Rights." *Penn State International Law Review*: Vol. 22: No. 1, Article 12.

Dowdell, John W. (2017). “An American Right to Be Forgotten.” Winter Vol. 52, Issue 2 *Tulsa Law Review*. 311.

Downes, David. (2001). The macho penal economy mass incarceration in the United States from a European perspective. Punishment and Society, 3(1), 61-80.

Dror, Yehezkel. (1957). Values and the Law. *The Antioch Review, 17*(4), 440-454. doi:10.2307/4610000

Faisal, Kamrul. (2021). "Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions." *Security and Privacy*, 4(4), 157.

Federal Communications Commission. April 20, 2016. "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." *Federal Register*, Vol. 81, No. 76.

Floridi, Luciano. 2015. "The Right to be Forgotten': A Philosophical View." *SSRN.*

Friedman, Matthew. November 15, 2015. "Just Facts: As Many Americans Have Criminal Records as College Diplomas." *Brennan Center for Justice Fact Sheet.*

Gajda, Amy. 2007. "What if Samuel D. Warren Hadn't Married a Senator's Daughter? Uncovering the Press Coverage that Led to The Right to Privacy." *SSRN*.

Gajda, Amy. (2015). *The First Amendment Bubble*. Harvard University Press.

Gibbs, Samuel. August 2014. "France requests most 'right to be forgotten' removals from Google." The Guardian.

Globocnik, Jure. (2020). "The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)." *GRUR International*, 69(4), 380-388.

Graves, Franklin, & Gabriel, Germain. (2020). "Right to Not Be Forgotten (Sometimes): Celebrity Privacy Rights in a Data-Driven World." *Landslide® Magazine*, 13(2).

Gullapalli, Vaidya. November 6, 2019. "The U.S. Has No Right to be Forgotten. But One News Outlet Has Been Weighing the Costs of the Internet's Long Memory." *The Appeal.*

Haber, Eldar. 2018. "Digital Expungement." *Maryland Law Review.* Volume 77, Issue 2, Article 3.

Hauch, Jeanne M. (1994). "Protecting private facts in France: The Warren and Brandeis tort is alive and well and flourishing in Paris." Tulane Law Review, 68(5), 1219-1302.

Herzog-Evans, Martine. 2011. "Judicial rehabilitation in France: Helping with the desisting process and acknowledging achieved desistance." *European Journal of Probation.* Vol. 3, No.1, 2011.

Kalven, Harry. (1966). Privacy in Tort Law: Were Warren and Brandeis Wrong? *Law and Contemporary Problems*, *31*(2), 326–341. https://doi.org/10.2307/1190675

Kantorowicz-Reznichenko, E. (2013). The 'Net-Widening' Problem and its Solutions: The Road to a Cheaper Sanctioning System. *Available at SSRN 2387493*.

Kim, Pauline. T. (2017). "Data-Driven Discrimination at Work." *William & Mary Law Review*, 58(3), 857-936.

Kirk, David S. and Sarah Wakefield. 2018. "Collateral Consequences of Punishment: A Critical Review and Path Forward." *Annual Review of Criminology.* Pg 171-194.

Krotoszynski Jr, Ronald. J. (2013). "The Polysemy of Privacy." *Ind. LJ,* 88, 881.

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

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

Lageson, Sarah. E. (2022). Criminal Record Stigma and Surveillance in the Digital Age. *Annual Review of Criminology*, 5, 67-90.

Lessig, Lawrence. 2006. "Code: Version 2.0." *Basic Books, Perseus Group.*

Leta-Jones, Meg. 2016. *Control + Z: The Right to Be Forgotten.* NYU Press.

Mantelero, Alessandro. 2013. "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'." *Computer Law & Security Review* Volume 29, Issue 3, June 2013, Pages 229–235.

Markesinis, B.S. Dec. 2009. "Foreign Law Translations." University of Texas at Austin School of Law, Foreign Law Translation, France. https://law.utexas.edu/transnational/foreign-law-translations/french/case.php?id=1254

Maruna, Shadd. 2011. "Judicial Rehabilitation and the Clean Bill of Health in Criminal Justice." *European Journal of Probation.* 3(1). 91-117.

Mayer-Schönberger, Viktor. 2009. "Delete: The Virtue of Forgetting in the Digital Age." *Princeton University Press.*

McMahon, Maeve. W. (1992). *The Persistent Prison?: Rethinking Decarceration and Penal Reform*. University of Toronto Press.

Meijer, Sonja, Harry Annison, and Ailbhe O'Loughlin. 2019. "Fundamental Rights and Legal Consequences of Criminal Conviction." *Oñati International Series in Law and Society. Hart Publishing.*

Mendels, Pamela. June 26, 1997. "Supreme Court Throws Out Communications Decency Act." *The New York Times.*

Meyer, David. April 23, 2019. "The privacy and antitrust worlds are starting to cross over." *International Association of Privacy Professionals (IIAP).*

Mitsilegas, Valsamis. 2015. "The Symbiotic Relationship Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice." *The New Journal of European Criminal Law.* Volume 6, Issue 4.

Moor, James H. (1998). "If Aristotle were a computing professional." *Computers and Society,* 28(3), 13-16.

Organization for Economic Co-operation and Development, OECD. 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."

Palmer, Chassen. 2020. "Celebrity Privacy: How France Solves Privacy Problems Celebrities Face in the United States." *California Western International Law Journal*, 50(1), 9.

Palmer, Vernon Valentine. (2011). "Three Milestones in the History of Privacy in the United States." *Tul. Eur. & Civ. LF*, 26, 67.

Pasquale, Frank. 2016. "Reforming the Law of Reputation." *University of Maryland Francis King Carey School of Law, Legal Studies Research*. No. 2016-3.

Prosser, William. (1960) Privacy. California Law Review, 48, 383-423.

Radamaker, Dallis. 1988. *The Political Role of Courts in Modern Democracies: Chapter 7, Legal Culture in France*. Macmillan Press, London.

Regan, Priscilla M. 2011. "Response to Bennett: Also, in defence of privacy." *Surveillance & Society* 8(4): 497-499. http://www.surveillance-and-society.org | ISSN: 1477-7487

Reichel, P. L., & Reichel, P. L. (1999). *Comparative criminal justice systems: A topical approach*. Upper Saddle River, New Jersey: Prentice Hall.

Reymond, Michel José. 2019. "The future of the European Union 'Right to be Forgotten.'" *Latin American Law Review* n.o 02, pg. 81-98.

Robertson, Adi. June 19, 2019. "Why the Internet's Most Important Law Exists and How People are Still Getting it Wrong." *The Verge.*

Rosen, Jeffrey. July/August 2012. "The Right to Be Forgotten." *The Atlantic.*

Rustad, M. L., & Kulevska, S. (2014). Reconceptualizing the right to be forgotten to enable transatlantic data flow. Harv. JL & Tech., 28, 349.

Satariano. Adam. (Sept 4, 2019). "'Right to Be Forgotten' Privacy Rule Is Limited by Europe's Top Court." *The New York Times.*

Scott, Mark. June 12, 2015. "France Wants Google to Apply 'Right to Be Forgotten' Ruling Worldwide or Face Penalties." *The New York Times.*

Silva, Lahny R. 2010. "Clean Slate: Expanding Expungements and Pardons for Non-Violent Federal Offenders. *University of Cincinnati Law Review.* Issue 155.

Solove, Daniel J. (2000). "Privacy and power: Computer databases and metaphors for information privacy." *Stan. L. Rev*., 53, 1393.

Solove, Daniel J. (2004). *The digital person: Technology and privacy in the information age.* (Vol. 1). NYU Press.

Solove, Daniel J. and Hartzog, Woodrow. 2013. "The FTC and the New Common Law of Privacy." *Columbia Law Review* 115, 583.

Stepanyuk, Mark. Feb 18, 2022. "Stratton Oakmont v. Prodigy Services: The Case that Spawned Section 230." *Washington Journal of Law, Technology, and Arts.*

Stone, Harlan. F. (1936). The Common Law in the United States. *Harvard Law Review*, 50(1), 4-26.

"The Concept of the Right to be Forgotten and the Analysis of the Results of Decision No. ECJ-131/12 Rendered by the European Court of Justice." November 12, 2019. *Mondaq*.

Toobin, Jeffrey. September 29, 2014. "The Solace of Oblivion." *The New Yorker.*

Vallas, Rebecca and Sharon Dietrich. 2014. “One Strike and You’re Out: How We Can Eliminate Barriers to Economic Security and Mobility for People with Criminal Records.” *Washington: Center for American Progress*.

Villaronga, Eduard. F., Kieseberg, P., & Li, T. (2018). “Humans forget, machines remember: Artificial intelligence and the right to be forgotten.” *Computer Law & Security Review,* 34(2), 304-313.

Warren, Samuel; Louis D. Brandeis. Dec. 15, 1890. “The Right to Privacy.” *Harvard Law Review*, Vol. 4, No. 5., pp. 193-220.

Waltman, Jerold L, and Kenneth M. Holland. 1988. *The Political Role of the Law Courts in Modern Democracies*. Macmillan Press, London.

Werro, Franz. 2009. “The Right to Inform v. the Right to be Forgotten- A Transatlantic Clash”
Georgetown Law, Center for Transnational Legal Studies Colloquium. Research Paper No. 2.

Westin, Alan F. (1968). “Privacy and freedom.” *Washington and Lee Law Review*, 25(1), 166.

Whitman, James Q. (2003). "The two western cultures of privacy: Dignity versus liberty." *Yale Law Journal.* 113: 1151.

Xue, M., Magno, G., Landulfo Teixeira P Cunha, E., Almeida, V., & Ross, K. W. (2016). The right to be forgotten in the media: A data-driven study. Proceedings on Privacy Enhancing Technologies, 2016(4), 389-402.

Zimmerman, Diane L. 1982. “Requiem for a heavyweight: A farewell to Warren and Brandeis's privacy tort.” *Cornell L. Rev*., 68, p.291.

Ziniti, Cecilia. (2008). “Optimal liability system for online service providers: how zeran v. America online got it right and web 2.0 proves it.” *Berkeley Technology Law Journal*, 23(1), 583-616.

Zittrain, Jonathan. (2008). “Privacy 2.0.” *U. Chi. Legal F*., 65.

Cases Cited

Olmstead v. United States, 277 U.S. 438(1928)

Melvin v. Reid (1931)

Sidis v. FR Pub. Corporation (1938)

New York Times v. Sullivan (1964)

Griswold v. Connecticut (1965)

Katz v. United States (1967)

Briscoe v. Reader's Digest Publishing Co. (1971)

Sipple v. Chronicle Publishing Co. (1984)

Roe v. Wade (1973)

Florida Star v. B.J.F. (*1989*)

Cubby, Inc. v. CompuServe Inc (1991, NY District Court)

Stratton Oakmont v. Prodigy (1995, NY District Court)

Zeran v. America Online (AOL) (1997, Virginia District Court)

Martin v. Hearst (2015)