

Claremont Colleges

Scholarship @ Claremont

CMC Senior Theses

CMC Student Scholarship

2021

Privacy-as-Property: A New Fundamental Approach to The Right to Privacy and The Impact This Will Have on the Law and Corporations

Sevion DaCosta

Follow this and additional works at: https://scholarship.claremont.edu/cmc_theses



Part of the [Business Law, Public Responsibility, and Ethics Commons](#), [Common Law Commons](#), [Constitutional Law Commons](#), [Privacy Law Commons](#), and the [Public Law and Legal Theory Commons](#)

Recommended Citation

DaCosta, Sevion, "Privacy-as-Property: A New Fundamental Approach to The Right to Privacy and The Impact This Will Have on the Law and Corporations" (2021). *CMC Senior Theses*. 2635.
https://scholarship.claremont.edu/cmc_theses/2635

This Open Access Senior Thesis is brought to you by Scholarship@Claremont. It has been accepted for inclusion in this collection by an authorized administrator. For more information, please contact scholarship@cuc.claremont.edu.

Claremont McKenna College

Privacy-as-Property:
A New Fundamental Approach to The Right to Privacy and The Impact This Will Have on the
Law and Corporations

Submitted to
Professor Paul Hurley

By
Sevion DaCosta

For
Senior Thesis
Spring 2021
May 3, 2021

Abstract

The most popular conception of the right to privacy stems from Warren and Brandeis's description of privacy as "the right to be left alone." This theory ultimately points to a more fundamental approach to the right to privacy rooted in property rights. This fundamental approach - which I call *privacy-as-property* - is what I establish in this paper. I argue that the Lockean concept of property that "every man has a property in his own person" provides the foundation for the right to privacy. *Privacy-as-property* begins with the fundamental right to control oneself. Because of this intrinsic right, your property right over yourself extends to your external property, including your cloud data. Since you control yourself, you cannot tacitly consent to giving your privacy away. Therefore, *privacy-as-property*, rejects the Lockean tacit consent argument. If one is not truly provided the freedom of choice to accept a set of agreements, then their right is not upheld. With this conception of privacy and the innate right to control oneself, when you select "agree" to use a third-party application, you do not tacitly consent to forego your right to privacy. This conception of privacy is then applied to help explain past SCOTUS cases, the implicit right to privacy in the Constitution, and regulatory changes. *Privacy-as-property* will eventually be codified in the law but there is a current market share, one that focuses on privacy that can be gained. Therefore, businesses will effectively alter their practices to align with *privacy-as-property*, before regulatory changes mandate it.

Table of Contents

Acknowledgements	4
Preface	7
Introduction: New Privacy Issues	10
Part 1: Establishing Privacy-as-Property	14
Chapter 1: Privacy. How do we define it?	14
Chapter 2: Moral and Legal Right to Privacy: Different but the Same	16
Chapter 3: Locke and Property	19
Chapter 4: The Right to Be Left Alone	25
Chapter 5: The Implicit Right to Privacy in the Constitution	29
Griswold v. Connecticut	32
Chapter 6: Privacy-as-property	36
Part 2: Technology, Tacit Consent, and Evolving Business Practices	38
Chapter 7: We're All Being Tracked	38
Chapter 8: Tacit Consent. Smith trumps Locke.	41
Chapter 9: The Carpenter's Rejection of Tacit Consent	46
Chapter 10: Data Aggregation: What Permits This?	52
Chapter 11: Why Businesses Are Not Entitled to Privacy-as-property	57
Chapter 12: Apple's Launch into <i>Privacy-as-Property</i> ?	62
Chapter 13: Conclusion	72
Bibliography	76

Acknowledgements

The list of individuals I would like to thank can be a thesis in its own right. I would like to extend my deepest, most sincere, and heartfelt gratitude to all those who have helped me along my various endeavors. Their support, mentorship, guidance, help, prayers, and encouragement have inspired me to follow my dreams, passions, and challenge myself. I will forever be a grateful for those who have entered my life and have helped me grow into the individual I am today. In all honesty, writing this acknowledgments section was the hardest part of completing my thesis. The list of individuals who I would like to thank spans hundreds long and I ultimately realized I would not be able to properly encapsulate the impact each individual has had on me, simply by listing their names. Therefore, to those that may not be listed below, you know the impact that you have had on me and the memories that we have made. You have all been paramount in contributing to what I have achieved at Claremont McKenna.

As I graduate from Claremont McKenna College and prepare for the next chapter in my life, I would like to thank the following individuals:

To Professor Hurley, thank you for being there every step of my College journey! It was a blessing having you appointed as my academic advisor and I am extremely grateful to also have you as my thesis advisor. Your advice, mentorship, humor, directness, and knowledge have been a tremendous help to me throughout my CMC career and during the thesis writing process.

To those at Berner Trail Jr Public School. Thank you for helping me to launch my academic passion and sports fascination. Mrs. Pappas, it all started with you. From grade one you always believed in me and saw my academic and leadership potential. I am forever grateful.

To Cheryl Lewis and all the rest of the individuals at ACCN. Thank you for the amazing work you have done for myself, and Black children all across Canada. Your impact will be span generations.

To the countless teachers, administrators, friends, coaches, Lang Scholars, and mentors during my time at Upper Canada College, I will forever be grateful for your wisdom, encouragement, and support. Mr. Blaire Sharpe, you were like a father figure to me. I will forever be grateful for your humor, kindness, and rugby coaching skills. English classes without you will never be the same. Mrs. Fiona Marshall, I am extremely grateful to have had you as a mentor, teacher, and mock trial coach. Your motivation and support allowed me to delve into my study of the Black Panther Party and blossomed my passion for law.

To the numerous professors, staff, and friends that I have made during my time at CMC. Thank you for your wisdom, advice, and support.

Marcie Gardner, your guidance and mentorship over the years have been invaluable. I would undoubtedly not be able to achieve what I had as President of the Mock Trial club if it wasn't for you. Amy Flanagan, and the RDS team, thank you for your help over the years as I have journeyed through differing career paths and found myself along the way. Mrs. Jennifer Hirsch, from my first interview with you in October 2016, I knew that CMC would be a place for me to thrive and excel at. Thank you and the rest of the admission staff for the hard work you do!

Professor Binay, your career advice and passion for your students was inspiring. Your classes launched my passion for finance. Lastly, to some of my closet friends, Cam, Jake B, Jake N, Josh, and Spence, thank you for challenging me, debating me, and pushing me to be better.

To my mentors over the years, Jordan Banks, Josh Keough, Jamie McDonald, Coach Steve Karam, thank you for always spending the time to have calls with me to discuss my future. For speaking candidly about your life experience and always connecting me with others to provide me a new experience. To Brittany Wielgosz, Aunty Britt, thank you for your continued support over the years. Jamie Shulman, from the first summer experience at Hubdoc you have been in my corner every step of the way, propelling my journey. To the Hutcherson's, Sue and Blake, thank you for your continued kindness and mentorship. There are not many people willing to drive someone an hour and half the day after a huge injury to a surgeon to ensure everything was okay.

To Robbie Pryde, Uncle Rob, I am deeply indebted to you for your kindness, mentorship and support over the years. It is hard to think that I would be able to accomplish what I have if it wasn't for you.

Family is the most important thing to me, and I would first like to thank my late grandparents. To my Grandpa, thank you for taking the leap of faith and moving to Canada from Jamaica to create a better life, with endless opportunities, for your family. I will never forget our time spent watching wrestling and the countless lessons you taught me over the years. To my grandma, Nana, thank you for coming over with gramps, and always speaking your mind - even when it was while Gramps and I were watching wrestling. Thank you for patience in teaching me how to love God as a young boy even if what I really wanted to do that Saturday morning was watch cartoons. Saying goodbye to you both was extremely difficult, but I know that you are with me every step of the way.

Aunty Sonia, thank you for teaching me how to lose. I will forever remember that day where you walked me after a loss in a soccer game, one that devastated me, and explained to me how to look past the losses. To your devotion to Christ and the wisdom you have imparted on me and the rest of the family. Aunty Kerry thank you for always being there along my journey. Our conversations never dulled and your support for me never wavered, you were like a second mother to me! Uncle Lundeen, thank you teaching me the game of chess, although I still can't beat you yet, I will one day. I have greatly appreciated your support over the years. Aunty Daphne thank you for your continued love, prayers, and support over the years. Aunty Sheryl, thank you for taking the time to come visit me in DC and I hope to one day gain a green thumb like you. Uncle Bas, I remember when I was amazed as a kid of your driving skills, specially driving in reverse. Tasha and Tricia thank you for your support, check-ins, and blessings over the years. To Alex, thank you for being a great cousin. I always looked forward to your visits in California and our food experiences. We'll have to head to Santa Monica again sometime soon. To all my other cousins, I always looked forward to our countless family events.

To my big bro, JeQuille, our journey has been one for the ages. I have looked up to you since day one. From our days of sneaking to watch TV when mom wasn't home, me constantly beating you in Madden, and weight room adventures our bond will never be broken.

To my nephew Elijah. Little man you are a bundle of joy. You motivate me to work harder every day. From our Sonic Adventures to Lego building, watching you grow has been profound. You are ridiculously smart and nothing I say gets past you! I can't wait to see what you do in this world.

Lastly, to my mother. Words cannot even express how grateful I am for you. Raising two Black boys as a single mother must have not been an easy feat, but you were always there for us. You have pushed me to follow my dreams, become a better version of myself, and to work harder. Your strength and wisdom are unmatched. Thank you for listening to me read countless papers, cover letters, and topics you had no interest in but did so to support me. Through every step of my journey, you have been there along the way. I love you mom.

Thank you, from the bottom of my heart, to everyone who made this thesis, and more importantly this journey, possible. I hope I made you proud. It is essential to never forget where you come from in life. And with that I leave you with my two favorite quotes:

“With man this is impossible, but with God all things are possible.” – Matthew 19:26

“There is nothing noble in being superior to your fellow man; true nobility is being superior to your former self.” – Ernest Hemingway

Preface

I was in high school when I first learned about the deeper conception of the right to privacy. My school Upper Canada College, at our annual World Affairs Conference, brought in Edward Snowden to be our keynote speaker.¹ Prior to this event in 2015 I had never heard of Edward Snowden and his whistleblower efforts. However, as I sat at home watching the live stream of Snowden speaking to a packed auditorium, I became aware of a new phenomenon. It was then in my senior year, as I was writing my extended essay for Mrs. Marshall on the Black Panther Party, I again arrived upon this topic of the right to privacy. This time it was through the lens of the COINTELPRO intelligence program used by the FBI to dismantle the Black Panther Party and other civil rights activist groups. These historical documents displayed detailed notes of surveillance efforts, data collection, and more.

When I arrived at Claremont McKenna this interest in privacy was amplified. Professor Hurley's Philosophy of Law introduced me to the Joel Feinberg's offense principle, which explained why we actually have privacy and ban certain actions in public. Then in my first semester of my Philosophy, Politics, and Economics major Professor Hurley introduced me to John Locke's *Second Treatise of Government*. It was through reading that text, where my foundation for my fundamental approach to privacy began. It simply made sense to me that privacy begins with property. The most innate form of property is your body and liberty to control that property is fundamental to be free. This fascination brought me to write a final paper, a paper in which I conceive of a framework for a fair criminal justice system. Privacy is essential

¹Upper Canada College, "Edward Snowden Speaks to World Affairs Conference 2015," YouTube, February 3, 2015, www.youtube.com/watch?v=JXplakuhjL8.

in the right to a fair trial, and I took this framework with me to the Public Defenders Service (PDS) in the District of Columbia.

In my role, I had the pleasure of working under a staff attorney - Amy Phillips - that cared immensely about her clients. In the course of working on difficult cases at PDS, my learnings about the law and legal theory came to life. I was protected by a shield of privacy, better known as the attorney-client privilege. Although I was simply an investigative intern, I was bound to this agreement. This foundation of the attorney-client privilege is inherently one in a property interest in oneself. The privileged information is now, and forever, the client's. They can disclose this information to help you work for them, but that information is never, for lack of a better term, owned by you. And this privilege never ends. This was important in my conception of privacy I have framed here. You own your information, you may share that information, but it's still yours. The attorney-client privilege may be different from our use of technology but they both require intimate data and disclosures. My experience with one client in particular, provided a valuable lesson that I never could have learned in the halls of Claremont. Consistent reliability and efforts to develop a relationship will eventually arrive in trust from your clients. This showed me that the first step towards securing a fair trial is building trust with one's client. However, whether or not I built trust does not change the privacy provided to a client in the attorney-client relationship. Whether or not that individual trusted me or simply reluctantly gave me that information, they were provided the same legal protection. This is where I arrived at the connection to my rejection of tacit consent that I make in this paper. In the world of technology, we are essentially forced to give our data to companies. Clicking "accept" on a terms and conditions, or cookies pop up, isn't truly a form of acceptance when your only options are accepting or not using. Lastly, my internship working at BlackRock in their Legal and

Compliance department allowed me to work on Material Nonpublic Information agreements. It was through working on these assignments that I got to add the last piece to my privacy puzzle. I saw how privacy spans across all industries, regions, and individuals. Therefore, my *privacy-as-property*, can span across international borders, jurisdictions, and apply to evolving technology. The right to privacy must be able to span across generations and I believe my conception will.

This thesis isn't simply a process of research and creation. It's a combination of all my past experiences, individuals I've met, relationships I've had and much more; it's a representation of how life experiences can influence a conception of privacy. I hope that you enjoy this piece and can ultimately see how *privacy-as-property* is the fundamental way to approach the right to privacy.

Introduction: New Privacy Issues

You can ask anyone if they have a fundamental right to privacy and they will tell you yes. If you were then to ask them what this privacy entails, they might provide you with examples of how society shares common tendencies of privacy. We close our room door to have some privacy, lock our home and close the blinds to prevent others from seeing into our private life. We add passwords to our phone to keep others out and even wear clothes to seemingly keep our private parts, private.

However, if you asked them where this right to privacy comes from, the answers become less certain. The word “privacy” does not appear anywhere in the United States Constitution. Nonetheless privacy is, and has been for many years, a heavily discussed concept. Privacy is by definition a personal right. It is commonly thought of as the right to exclude others from accessing your information or the right to separate yourself from others.² Although this form of privacy is not explicitly set out in the Constitution, it is derived from the broader concept of “liberty” and is therefore somewhat harder to define and a bit more controversial.³

The issues regarding the right to privacy have become more vital today as more of our inherent privacy is currently under siege due to new technological advancements. It is hard to fully grasp the threat to privacy today, but the trade-off between privacy and convenience has threatened the right to privacy like we have not seen before. The new technological innovation of smartphones, smart assistants, social media, and big data, require that we must re-establish the right to privacy in light of these advancements.

² Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age*, (Cambridge: Cambridge University Press), 26

³ Ellen Alderman and Caroline Kennedy. *The Right to Privacy*. (New York: Vintage Books, 1997), XV

The legal and scholarly world has attempted to conceptualize and codify in the law the inherent right to privacy. The legal authorship of the right to privacy began in 1890, when Justice Louis Brandeis and attorney Samuel Warren quantified the right to privacy as the “right to be left alone.”⁴ This idea is what first comes to mind when many people think about the right to privacy.⁵ However, this interpretation points to a more fundamental approach to the right to privacy that is rooted in property rights. What I will establish in this paper is that the desire for privacy, private property, is best understood as the ability to have control over one's own person. This fundamental approach to the right to privacy will be described as *privacy-as-property*. This *privacy-as-property* theory establishes, using the Lockean conception of property, that privacy starts with the fundamental right to control oneself.

This conception will be essential when arriving at discussions regarding tacit consent, third-party doctrine, changing laws and current business practices. In this technology age, some may believe that when we “agree” to share something - whether that’s an email address with a rewards program or signing up for a social media account - that we no longer have control of this information.⁶ As a consequence, because we “agreed” to the terms and conditions, we have foregone our privacy right over the use of this data. My conception of privacy will vehemently reject these claims. It will establish that in the age of technology sharing information is, many times, involuntary and unavoidable. Therefore, the exact reason - under our current legal framework - for why we share information has no bearing on your right to privacy. As will be

⁴ Samuel D. Warren and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review*, vol. 4, no. 5, (1890): 193–220, www.jstor.org/stable/1321160

⁵ Jack Hirshleifer, "Privacy: Its Origin, Function, and Future." *The Journal of Legal Studies* 9, no. 4 (1980): 649-64. <http://www.jstor.org/stable/724176>.

⁶ Waldman, *Privacy as Trust: Information Privacy for an Information Age*, 3.

established, we are not tacitly consenting to forego our right to privacy and that is because we must view *privacy-as-property*.

With the vast innovation seen over the past decade, newer challenges regarding ways to protect privacy have posed new challenges to lawmakers. How exactly can one balance the convenience that these new technologies provide us in our daily life with the personal privacy that should be afforded to each individual. What is the right to privacy that each individual has? This question is one that is not new but still poses challenges to this current day. However, there are no other rights without the right to privacy. Understanding how to truly approach the right to privacy is essential in not only furthering our privacy protections but also for individual liberty.

The first part of this thesis will focus on establishing the conception of *privacy-as-property*. It will begin with a brief discussion of common definitions of privacy, before delving into the moral and legal implications of privacy frameworks. In order to establish that privacy rights come from the right to control our own property, it is then essential to look at the founding of the idea of property rights. Therefore, I will then establish the Lockean conception of property rights and how the innate right to control oneself applies to privacy rights. With the Lockean conception established, we can then discuss Warren and Brandeis's right to privacy, known "as the right to be left alone." Although their theory was foundational to future privacy discussions, they didn't quite establish the connection to *privacy-as-property* that I will. To highlight these discrepancies, I will present a case for privacy being both implicit and explicitly detailed in the United States Constitution and look at past Supreme Court (SCOTUS) cases. Once we conclude this, my conception and application of *privacy-as-property* will be clear.

The second part of this thesis will then discuss how *privacy-as-property* rejects the Lockean tacit consent argument and instead provides a clear directive for how privacy should be

codified in the law. Moreover, I will establish that this conception of privacy can explain the inevitable market pressure that businesses will face and have started to see. Competition will force businesses to focus on privacy before the law mandates them to. Considering that fact, I concluded will a discussion of Apple's new privacy feature, App Tracking Transparency, and how it is best explained through *privacy-as-property*.

This conception of *privacy-as-property* will span generations and will remain fundamental sound with further advancements in technology.

Part 1: Establishing Privacy-as-Property

Chapter 1: Privacy. How do we define it?

When one searches for a definition of privacy in the Oxford Dictionary the first definition appears as follows: *noun* “*The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.*”⁷

The etymology of the word privacy is derived from the Latin adjective *privus*, the original archaic meaning being “single.”⁸ This origin makes it evident why, when we define privacy, we conceptualize it as the ability to exclude others, hide secrets, or liberty to be left alone. Warren and Brandeis, as I will later discuss, use this approach when discussing their conception of privacy: “the right to be left alone.”

If you search for the word private, you arrive at this definition: *adj* “*Restricted to or for the use or enjoyment of one particular person or group of people; not open to the public.*”⁹ This definition is what we commonly think of when we speak of private property. The origin for this can be derived from two Latin words: *privatus*, “which refers to the withdrawal from public life or the separation from others” and *privare*, of “privation and deprivation”¹⁰ help to establish the suggestive nature of privacy. When we usually consider private property, we think about having ownership, property, in things.

However, the Lockean perspective establishes property as a much broader notion. One is not granted privacy and then private property; instead, privacy is property, the right to control

⁷ "privacy, n.". OED Online. March 2021. Oxford University Press. <https://www-oed-com.ccl.idm.oclc.org/view/Entry/151596?redirectedFrom=privacy>

⁸ Hirshleifer, "Privacy: Its Origin, Function, and Future," 649-64.

⁹ "private, adj.1, adv., and n.". OED Online. March 2021. Oxford University Press. <https://www-oed-com.ccl.idm.oclc.org/view/Entry/151601?rskey=nxnp5c&result=1&isAdvanced=false>

¹⁰ Waldman, *Privacy as Trust*, 25

yourself, and your personal space. Therefore, the right to privacy begins with the fundamental right to control one's own person. The most fundamental form of property. One cannot ask to be left alone without an understanding why one has the right to control oneself.

Take for example if an individual entered your home and did not steal or destroy anything, instead they made your bed. This action, although you were left alone, would still constitute a violation of your right to privacy. Why is that? The reason is that it stems from your innate right to control your person, which is extended to your external property, in this case your house. Therefore, your right to privacy was violated whether or not the action by the perpetrator was harmful. The only way to truly define the right to privacy is through the innate right one has over oneself.

Chapter 2: Moral and Legal Right to Privacy: Different but the Same

It is important to note that the right to privacy can be thought of as either being a moral or legal right. There are key cases in which the violation to the right to privacy has resulted in legal recourse. This involves overturned convictions, civil lawsuit payouts, and changing business practices. The Supreme Court has discussed a multitude of privacy issues as they pertain to reasonable searches, marriages, contraception, and the use of cell phone data. Ellen Alderman and Caroline Kennedy break down these legal areas in their book *The Right to Privacy as: Privacy v. Law Enforcement, Privacy and Your Self, Privacy v The Press, Privacy v. The Voyeur, and Privacy in the Workplace.*¹¹ These are just some of the legal ways that privacy can be conceived. Others may include the protection granted to students through the Family Educational Rights and Privacy Act, or the Right to Financial Privacy Act which protects financial holdings, the Video Protection Privacy Act, and the Health Insurance Portability and Accountability Act.¹² Any direct breach of these contracts can, more likely than not, result in legal recourse.

The other aspect of the right to privacy involves moral judgment which involve violations to an individual's right to privacy. These can include when a friend tells your deepest secret to someone else or when someone reads your diary. There are undoubtedly harms felt when someone does not respect your secrets and intimacy - when someone doesn't respect your right to privacy in these examples - but it is harder to codify in the law. Let's consider a hypothetical scenario:

¹¹ Alderman and Kenny, *The Right to Privacy*.

¹² Waldman, *Privacy as Trust*, 20 – 21, 157 -158

If I were to ask you, the current reader, to text me the password to your email right now many of you would not. That's because you would prefer to keep that information private and to yourself. However, there may be a few of you that decide you're okay with sending that information. Nonetheless, whether or not you opt-in or opt out, to sending me your password, if I walked by you and automatically gained access to your email, this would violate your right to privacy. As you have not willingly given up your personal information. I would then have uncontrolled access to your private emails, conversation, and a glimpse into your life without your consent to read these documents. That is a key distinction in the world of privacy. One can choose to not provide access to their personal information but one can also opt-in to sharing that information. However, in the new world of technology more often than not those in the first camp - of not wanting to share their personal information - are not tacitly consenting to giving away their privacy. In essence, as we conduct our daily life, our right to privacy is not being upheld. This example presents both an illegal act - as I gained access to your close contacts and private information - and a moral harm - I caused you wrong as you did not provide me with the right to search your emails.

On the other hand, if you were to tell your friend about an extremely embarrassing story and ask them to keep it a secret and they didn't, that would only violate your moral right not your legal protected right. Although, this example will not require legal recourse, it is still a violation of your fundamental right to privacy. A right, for the purpose of this paper, can be defined as "that which is considered proper, correct, or consonant with justice, and related uses."¹³

Not all privacy violations rise to the level at which society, through the legal system, becomes involved; some are just gossip and acts of faithless friends, which the law can do

¹³ "right, n." OED Online. March 2021. Oxford University Press. <https://www-oed-com.ccl.idm.oclc.org/view/Entry/165853?rskey=NxBaAs&result=1>

nothing about.¹⁴ Some legal violations of the right to privacy may very well be moral violations;¹⁵ but moral violations may not be legal violations. There is also a qualitative difference between an invasion of privacy by your government and an invasion by a stranger.¹⁶ Nonetheless, whether the courts are involved or not, these intrusions all violate the right to privacy that will be established.

Therefore, this paper will establish the right to privacy that includes both the moral and legal sense to the right to privacy. And specifically, how the right to privacy should be codified in the law.

¹⁴ Alderman and Kenny, *The Right to Privacy*, The Right to Privacy, XV

¹⁵ Consider the moral and legal violation of the right to privacy found in revenge porn cases. This violates your right to privacy because you have not tactically consented to foregoing your right to control that video simply because you made it with, or for, someone else. One cannot freely share that information. You do not tacitly consent to the other party having the ability to freely disseminate your video or pictures as they please. This is why revenge porn cases are both legally and morally reprehensible violations to the right to privacy.

¹⁶ Alderman and Kenny, *The Right to Privacy*, The Right to Privacy, 13

Chapter 3: Locke and Property

The de facto possession of physical property is not enough to truly understand the impact property rights have on the right to privacy. One can find in nature, a complementary reluctance to intrude.¹⁷ Internalized respect for property is what permits autonomy - freedom to do as you please - to persist within society.¹⁸ As Jack Hirshleifer explains “all known primitive communities have been found to possess relatively elaborate structures of property rights.”¹⁹ Therefore, all territorial species must be proprietors, who defend their territories and ward off incursions on their fundamental right, the right to privacy.²⁰ This is why property rights play an important role in establishing the right to privacy; people want to protect their property from others. The concept of controlling one's property is intertwined with the concept of privacy. When considering their interconnectedness, it is essential to start with the Lockean perspective on property rights.

John Locke, an English philosopher and physician, developed - in his *Second Treatise of Government* - a theory of property that is essential for understanding the right to privacy. Locke establishes his original property principle by detailing that “every man has a property in his own person”²¹ and this right is one that “nobody has a right to, but himself.”²² What this means is that no matter the country, or laws that govern your state, privacy is first and foremost an extension of your person. The ability for one to have fundamental liberty, begins with having control over one's person (property). This concept is necessary for the claim that the right to privacy begins

¹⁷ Hirshleifer, "Privacy: Its Origin, Function, and Future," 649-64.

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.

²¹ John Locke, *Second Treatise of Government*, (1980) Edited by C. B. Macpherson. Cambridge, MA: Hackett Publishing, Sect, 27.

²² Ibid.

with the fundamental right to one's person. The rights in which you have over yourself means that self-ownership lends itself to allow you to have the right to privacy in all of your external possessions. Therefore, the first fundamental right to property, the right to control oneself, naturally extends to all other objects which you own.

However, this claim seems at first glance to not answer the question of why we can consider *privacy-as-property*. Why does this right to have property over your person naturally extend to other items that we constantly use and own, such as phones, homes, cars, and journals. Well, the answer for this is contained in Locke's labor theory of property. Locke equates labor with property rights stating that "it is very easy to conceive, without any difficulty, how labor could at first begin a title of property in the common things of nature."²³

Though the Earth, and all inferior Creatures be common to all Men, yet every Man has a Property in his own Person. This nobody has any right to but himself. The Labour of his Body, and the Work of his Hands, we may say are properly his. Whatsoever then he removes out of the State that Nature hath provided, and left it in, he hath mixed his Labour with, and joined to it something that is his own, and thereby makes it his Property.²⁴

This concept was essential to early American Courts discussions regarding property cases between Native Americans and European Settlers. If one decided to build up the land, it was then their property. The early Court's decisions seemed to agree with this idea when they sided with the European settlers and not Native Americans. The Europeans built fences on their land, but the Native Americans treated their land respectfully as to not destroy it by building large houses. This solidifies Locke's larger argument that humans - beginning in a state of perfect freedom²⁵ - have the autonomy to live as we choose, so long as we are not violating or interfering with

²³ Locke, *Second Treatise of Government*, Sect. 51

²⁴ *Ibid*, Sect. 27.

²⁵ *Ibid*, Sect. 34.

others. For Locke, people were created with reason from God which allowed us to use our right to control ourselves, to create property through our labor, while respecting others property rights.²⁶ Despite land first being viewed as a common good,²⁷ anyone who now cultivates that land, alters it in a distinct way, as Locke would describe it puts it, “mixed his Labour with, and joined to it something that is his own, and thereby makes it his property.”²⁸ Because we now own this property, we have the ability to prevent others from entering;²⁹ we have then created our own privacy through property.

Thus, this labor conception of property is profoundly connected to the right to privacy. Locke has provided us with a key foundation. Because we own ourselves (property), we can mix our labor with land to create privacy and exclude or allow others to enter our property. Thus, establishing our right to privacy, *privacy-as-property*. If we can do this with physical property, or extrinsic objects, we then are allowed to have the right to privacy for our most fundamental property, our bodies. This will then include the right to share your personal information, consent to others seeing your body, enter your home, and more. This accompanying choice, whether or not to share, is integral in securing the right to privacy. This labor theory changed property law forever and its applications to conception of privacy are profound.

Furthermore, Locke's perspective on money strengthens the labor theory's application to modern day privacy. The original establishment of labor granting you property did not include a form of payment. Thus “the labor that was mine, removing them out of that common state they were in, hath fixed my property in them.”³⁰ Therefore, in this time period the idea of

²⁶ Locke, *Second Treatise of Government*, Sect. 25-28, 31, 63.

²⁷ *Ibid*, Sect. 25, 28.

²⁸ *Ibid*, Sect 26-28.

²⁹ Waldman, *Privacy as Trust*, 14

³⁰ Locke, *Second Treatise of Government*, Sect. 28.

accumulating too much food or land could lead to waste as you would be unable to utilize labor over each excess land or store additional food. Leading to you losing your land and it returning to a common pool (for someone else to labor over).³¹ So labor doesn't necessarily equate to owning all property, under the Lockean perspective, they own the labor that they can maintain and cultivate. Without a form of payment, one only had control, or the right to privacy over their own person, and land or items that they were laboring over. Thus, the introduction of money, an item that never spoils and can continually be accumulated, altered the ability for one to waste property.³² One was now able to enlarge their possession of land more than their family needed and no one could take their land even if they "wasted" portions of it.³³

"By a tacit and voluntary consent, found out a way how a man may fairly possess more land than he himself can use the product off.... By putting a value on gold and silver, and tacitly aggressing in the use of money: for in government laws regulate the right of property, and the possession of land is determined by positive constitutions."³⁴

The meaning of waste differs greatly from our current day understanding. Many goods bought during the Lockean time period were easily perishable, but the majority of items we buy now have a long shelf life. Say you buy an iPhone with 512 gigabytes of storage. You however only use 100 gigabytes. I may think that you are wasting this space, but it in no way gives me the right to take, or labor, the remaining 412 gigabytes of storage your phone because you're not using it to its full capabilities. You have the right to privacy over your property that you have own.³⁵ In this light having an unused room in a mansion count is no more wasteful than having a

³¹ Locke, *Second Treatise of Government*, Sect. 27 and 42; Connections to this labor theory can be found in squatters' rights.

³² Ibid. Sect 37 and 47-50.

³³ Ibid. Sect. 48

³⁴ Ibid. Sect 50

³⁵ Whether this acquisition came through purchasing or it being gifted.

book for one hundred years that you only read once; and they both encompass the same right to privacy that governs your fundamental right to privacy. This is because instead of mixing our labor with land, we now labor to receive monetary compensation, which in terms allows us to purchase external items. Making these items our property because we have now mixed our labor with these purchased goods.

Locke argues that you have the right to property due to labor, it is the preservation and protection of that property that people desire.³⁶ This is where the full application of Locke's fundamental right to privacy is established and extends to our current day. Thus, Locke goes on to argue that man will leave the state of nature to receive the benefits of a social contract to increase the security of one's life, liberty, and property.³⁷ We as a society are able to agree on the use of monetary exchanges and even government laws to help protect our pre-established fundamental right to privacy over ourselves (internal) and our property in items (external). We then arrive back to the beginning of this chapter, and the fact that internalized respect for property is what permits autonomy - freedom to do as you please - to persist within society.³⁸ In this description of Locke, I have established 1) the fundamental right to privacy as a form of property in oneself, 2) that money allows you to own more property than you would need, thus increasing our property interest from simply ourself to all that we have mixed our labor with, and lastly 3) individuals want preservation and protection of their property and that will require contractual agreements.

³⁶ See paragraph one of this chapter.

³⁷ Locke, *Second Treatise of Government*, Sect 6, 22, 42, 57, 59.

³⁸ Hirshleifer, "Privacy: Its Origin, Function, and Future," 649-64.

I then arrive at a conclusion that although Locke does not discuss the explicitly detail relationship between individuals and privacy, he establishes the importance of property rights, which forms our understanding of the fundamental right to privacy.

Privacy-as-property as understood by our Lockean perspective encapsulates that one's property is governed by the fundamental right to privacy whether or not you are in physical possession of that property. Since my original labor prevented you from gaining access to that land (or property) my right to privacy imposes a restriction on your ability to simply do as you please without violating my unalienable fundamental right to privacy. You will always be in possession of your own body, the first form of property you have, and this principle extends to all of your other property.

As I have now established the fundamental right to privacy, and how it extends beyond just your physical person, we can now turn to the Justice Louis Brandeis and attorney Samuel Warren and their conception of privacy as “right to be left alone.”

Chapter 4: The Right to Be Left Alone

Warren and Brandeis are touted as bringing forth the first explicit definition of the right to privacy in the United States. However, their theory simply points to a more fundamental approach to the right to privacy rooted in property rights. Warren and Brandeis faced a challenge in their time similar to the vast technological advancement we are currently experiencing. In our modern day it is social media and artificial intelligence. But for them it was instantaneous photographs and newspaper enterprise invading the sacred precincts of private and domestic life, which necessitated, in their opinion, a new step to protect individuals.³⁹ It was their opinion that “the existing law affords a principle which can properly be invoked to protect the privacy of the individual... [and] if it does, what the nature and extent of such protection is.”⁴⁰ For Warren and Brandeis the right to privacy, as established through the common law, was simply the right of the individual “to be left alone.”⁴¹ This right to exclude others from our “thoughts, sentiments, and emotions” stemmed from the - the propriety endowed to us as autonomous individuals through our “inviolable personality.”⁴²

The distinction here is that Warren and Brandeis did not see the implicit understanding of the right to privacy embedded in the constitution.⁴³ Instead, they believed that it was necessary for the common law to establish the right to privacy. The common law “enabled the judges to afford the requisite protection [of one’s privacy], without the interposition of the legislature.”⁴⁴

³⁹ Warren and Brandeis, “The Right to Privacy,” 195

⁴⁰ Ibid, 197.

⁴¹ Ibid, 205.

⁴² Ibid, 193 & 196.

⁴³ I will discuss the role of the constitution further in the next chapter.

⁴⁴ Warren and Brandeis, “The Right to Privacy,” 195

Warren and Brandeis, view the concept of slander and libel as extended protection surrounding the physical property.⁴⁵ As well, they establish that no one has the right to publish one's productions in any form, without their consent.⁴⁶ This is an important aspect, that when applied to Locke's property rights displays the fundamental right to privacy that extends to your external items, in this case signs, painting, sculptures, music or words.⁴⁷ After a careful review of the *Prince Albert v. Strange* case, it is clear that Warren and Brandeis arrive at the ultimate conclusion that protection, the right to privacy, stems from the general right of the individual to be left alone.⁴⁸

However, Brandeis and Warren seem to be making a key mistake in their theory. They are claiming that privacy isn't property; but then what is it? For Brandeis and Warren, privacy is somewhat of a cautionary tale, something that stems from the right to be left alone, and aspects that are embedded in tort law. Warren and Brandeis begin with the notion that privacy isn't property; but then they discuss key cases such as *Prince Albert v. Strange* that displays the key intersection between property and privacy. Due to this misconception, they assume throughout their essay that property is stuff, but at the same time what they're truly calling property is the right to control oneself. Privacy, "the right to be left alone" is the really the right to control yourself. The property that is most fundamental is one's own self. Therefore, privacy is a property interest in controlling yourself. The way that Brandeis and Warren create their account makes it impossible for them to arrive at a clear account of privacy. This is due to privacy being in contrast with property. Instead, they should be seen as one in the same. Therefore, if you are able to see privacy as property in yourself, then all of the examples they discuss, photographing

⁴⁵ Warren and Brandeis, "The Right to Privacy," 197.

⁴⁶ *Ibid*, 199.

⁴⁷ *Ibid*.

⁴⁸ *Ibid*, 205.

without permission, publishing private letters, are going to be violations in your fundamental property interest, and thus a violation to your privacy. Privacy is the right to control yourself; what Warren and Brandeis detail as property is really to ability to control yourself. Which is an extension of having a property in yourself. The right to control oneself should be up to you, and you must consent to what is put out in the public domain. Therefore, the “to be left alone,” is not possible if you do not first have the ability to control yourself.

Let's consider an example where you are asleep, and a random individual has broken into your house and is sitting at the foot of your bed. In this situation that individual is violating both your personal space and, as a by-product of their trespassing, is violating your privacy by entering into your house without consent. If we simply apply the Brandeis and Warren doctrine regarding the right to privacy, this individual has violated your privacy simply because you have a right to be left alone and they are not leaving you alone. However, what if they were 50 feet away from your house and were instead hearing everything occurring in your home through a listening device. If we again apply the Brandeis and Warren doctrine it would seem like this individual has not violated your right to privacy because, technically, they are leaving you alone. When you apply *privacy-as-property*, you will see that, unlike Brandeis and Warren this is a violation of your right to privacy. This is because privacy is a property interest in oneself, and which stems from the ability to control oneself. Someone, who may be “leaving you alone” but is listening your conversation is clearly invading your right to privacy. The right to privacy is not just about violating your physical property, because in this case using a listening device didn't violate your physical space but instead your personal space. With technology one can violate your space without being there, or you even knowing, but the reason why this violates your right

to privacy is because you have the right to control your own property, and this action prevented you from having that choice.

Let's take a look at a case that used Warren and Brandeis's conception of privacy to reach a decision. What will become clear is that this court, ruling in the common law just more than a decade after Warren and Brandeis article ruled in a way that strengthens my conception of the right to privacy, not there's. In 1905 the Georgia Supreme Court updated state common law to provide a legal remedy for cases that involved an invasion of privacy. The case *Pavesich v. New England Life Insurance Company* dealt with an insurance company's newspaper advertisement using a photo of Pavesich without his consent. Pavesich sued and the Georgia Supreme Court ruled in their opinion that: "derived from natural law... the body of a person cannot be put on exhibition at any time or at any place without his consent . . . It therefore follows . . . that a violation of the right of privacy is a direct invasion of a [long-standing] legal right of the individual."⁴⁹ The Court's ruling can best be explained by *privacy-as-property*. Because Pavesich has the ability to control himself, he must provide consent to others who choose to use a photo of him. If there was no property interest in controlling oneself then there would be no privacy protection. However, as *privacy-as-property* established, there is property interest in oneself, that requires the ability to controlling oneself and all other owned property.

⁴⁹ *Pavesich v. New England Life Ins. Co.* - 122 Ga. 190, 50 S.E. 68 (1905)

Chapter 5: The Implicit Right to Privacy in the Constitution

The detailed Lockean perspective that has been established was extremely influential in helping to draft the constitution of the United States. Look no further than the most famous lines of the Declaration of Independence “unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.”⁵⁰ Locke himself wrote that there are unalienable rights to “life, liberty, and possessions.”⁵¹ The commonality between these two is that liberty must be understood as the right to privacy. One of the founding fathers James Madison’s ideas regarding property detail the similarities to the Lockean principle and establish the implicit existence of the right to privacy in the constitution. Privacy was essential in aiding the creation of the Constitution. However, you will not find the word “privacy” in the US constitution. So how does the Constitution ensure the right to privacy? The constitution provides a commitment to freedom; after all it was created following a time of rebellion. When understanding the constitution, it is grounded in the deepest traditions of liberal thought. Liberty in one's person, one’s right to control one's own person, is necessary to be free. Therefore, the goal of individual freedom is not possible without the right to privacy. The ability to have control over oneself and be free from external rule, *privacy-as-property*, played a key construction of the constitution.

So, one may ask, why did the Founders explicitly endorse specific aspects of privacy? Well, the answer is that one cannot have liberty without the right to privacy. Privacy in its broadest sense was already understood, but because of foreign rule there was a requirement to establish some specific liberties that were included in the general right to privacy. These include those more specific guarantees, found in the First, Fourth, Fifth, Sixth, and Ninth Amendment.

⁵⁰ Declaration of Independence, <https://www.archives.gov/founding-docs/declaration-transcript>

⁵¹ Locke, *Second Treatise of Government*, Sect, 59, 87, 135.

The framers were simply making explicit what was already implicit in the constitution. Let us take the Sixth Amendment as an example, one can see that the Sixth amendment is an explicit statement regarding one aspect of the right to privacy. More specifically one of the most intriguing aspects of the Sixth amendment is the right to counsel, which provides attorney-client privilege; but has also been understood over the years as meaning the right to *adequate* counsel. What was understood as time progressed was that simply having a physical attorney present did not uphold the true right granted to a defendant. Therefore, the Courts have established that the most reasonable interpretation of the right to counsel, is that a condition of adequacy of counsel is presupposed. The necessity of adequate was not explicit, but it was implicit. In the same light that the general right to privacy is not written in the constitution, albeit still present.

The creation of the Fourth amendment regarding reasonable search and seizure cannot be conceived without the understanding that the fundamental right to privacy is found in one's ability to control one's own person. Free from external intrusion, and to have the right to control oneself. The fourth amendment is the most direct constitutional protection of the right to privacy. The amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."⁵² The Supreme Court has held that this amendment protects an individual's "reasonable expectation of privacy."

The addition of the fourth amendment in the original constitution arose from an opposition to the "writs of assistance" used by officers of the Crown against the colonists in the New World.⁵³ The writs were general warrants that allowed officers to enter private property and "conduct a dragnet search for smuggled goods."⁵⁴ This law allowed British officers full

⁵² US Constitution, Fourth Amendment

⁵³ Alderman and Kenny, *The Right to Privacy*, The Right to Privacy, 10

⁵⁴ Ibid.

discretion to search property because they did not have to declare exactly what they were looking for and why.⁵⁵ The Fourth amendment was created to prevent those abuses power. James Otis Jr said at the time that “the use of writs places the liberty of every man in the hands of every petty officer.”⁵⁶ The Founders instated this right of “protection against unreasonable searches and seizures,” and required warrants to conduct a search. These warrants must be based upon “probable cause, describing the place to be searched and the persons or things to be seized.”⁵⁷ Above all, these searches must also be reasonable, and require justification for why the need to search outweighs the invasions of privacy that search encompasses. The framers made explicit the privacy protection granted in the fourth amendment as it safeguards “searches and seizures.”

This explicit protection is derived from the implicit fundamental privacy protection - property right in yourself. Liberty, as detailed in the Constitution, includes the fundamental right to privacy. The reason why the US made explicit what was already implicit was because it was explicitly taken away from the British. However, simply because they made a portion of the right to privacy explicitly does not alter in any way the implicit conception. If I tell you that we have to go to the store on either Tuesday or Thursday, and you respond saying that you don't want to go on Tuesday, you have now implicitly agreed to go on Thursday. But you can also make it explicit, and say I want to go on Thursday. It does not change the day we go, only the way in which you expressed that desire. This is the same with the right to privacy in the constitution. It was understood by Madison that the Lockean perspective that a property interest in oneself provided the foundation for liberty. There is no freedom without privacy.

⁵⁵ Alderman and Kenny, *The Right to Privacy*, The Right to Privacy, 10

⁵⁶ *Ibid*, 11.

⁵⁷ *Ibid*, 11.

This term [property] in its particular application means “that dominion which one man claims and exercises over the external things of the world, in exclusion of every other individual.” In its larger and juster meaning, it embraces everything to which a man may attach a value and have a right, and which leave to every one else the like advantage. In the former sense, a man’s land, or merchandize, or money is called his property. In the latter sense, a man has a property in his opinions and the free communication of them...He has a property very dear to him in the safety and liberty of his person. He has an equal property in the free use of his faculties and free choice of the objects on which to employ them. In a word, as a man is said to have a right to his property, he may be equally said to have a property in his rights.⁵⁸

The fourth amendment is to privacy what habeas corpus is to establishing justice; even an originalist must see the right to privacy as embedded in the constitution. The right is encoded in the law and extends to govern moral privacy. To look more closely at moral privacy, we can consider the case of *Griswold v. Connecticut*.

Griswold v. Connecticut

In 1879, Connecticut passed a law that banned the use of any drug, medical device, or other instrument in furthering contraception and made it a criminal offense for anyone to give information or instruction on their use. A gynecologist at the Yale School of Medicine, C. Lee Buxton, opened a birth control clinic in New Haven in conjunction with Estelle Griswold, who was the head of Planned Parenthood in Connecticut.⁵⁹ They were convicted of dispensing such information to married persons in violation of the law and fined \$100. The main legal question at hand in this case was whether the Constitution protects “the right of marital privacy against

⁵⁸ James Madison, *Property* (1792), Volume 1, Chapter 16, Document 23 <http://press-pubs.uchicago.edu/founders/documents/v1ch16s23.html>, The University of Chicago Press

⁵⁹ *Griswold v. Connecticut*, 381 U.S. 479 (1965), <https://supreme.justia.com/cases/federal/us/381/479/#tab-opinion-1945663>

state restrictions on a couple's ability to be counseled in the use of contraceptives?"⁶⁰ In a 7-2 decision for *Griswold*, Justice William O Douglas wrote the majority opinion of the court birthing the idea of "penumbras" for establishing the right to privacy. The opinion created the *stare decisis* that a general right to privacy can be inferred from the penumbras, created by specific guarantees of several amendments in the Bill of Rights, and this right prevents states from making the use of contraception by married couples illegal. The majority opinion used examples of certain rights that have become explicit in daily life that were not written in the constitution to display the implicit rights to privacy via penumbras in the constitution. Douglas went on to illustrate examples based upon the First, Third, Fourth, Fifth, and Ninth Amendments and their role in creating the penumbra from which the right to privacy must be inferred.⁶¹

Justice Douglas stated that "the association of people is not mentioned in the Constitution nor in the Bill of Rights. The right to educate a child in a school of the parents' choice—whether public or private or parochial—is also not mentioned. Nor is the right to study any particular subject or any foreign language. Yet the First Amendment has been construed to include certain of those rights."⁶² The Third Amendment, as described by Douglas, and its prohibition against the quartering of soldiers "in any house" in a time of peace without the consent of the owner is another facet of that privacy.⁶³ The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."⁶⁴ The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which the government may not force him to surrender to his detriment.⁶⁵ The

⁶⁰ *Griswold v. Connecticut*, 381 U.S. 479 (1965).

⁶¹ *Ibid.*

⁶² *Ibid.*

⁶³ *Ibid.*

⁶⁴ *Ibid.*

⁶⁵ *Ibid.*

Fourth and Fifth Amendments were combined to serve as a general protection against all governmental invasions “of the sanctity of a man’s home and the privacies of life.”⁶⁶ Lastly, for the majority opinion the Ninth Amendment provides “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”⁶⁷

However, not everyone on the court agreed with the penumbra argument in terms of the right to privacy. In fact, the right to privacy that is being established in this paper does not require an argument of penumbra as discussed in the prior section regarding the implicit constitutional right to privacy. The courts own account of the third amendment and the necessity of consent from an owner strengthens the conception of *privacy-as-property*.

Justice Goldberg detailed in his concurring opinion that the right to privacy was not contained in imaginary penumbras, but instead can be found in the Ninth and Fourteenth Amendments. The interpretation by Goldberg aligns more closely with this paper's established right to privacy. Justice Goldberg stated that the “language and history of the Ninth Amendment reveal that the Framers of the Constitution believed that there are additional fundamental rights, protected from governmental infringement, which exist alongside those fundamental rights specifically mentioned in the first eight constitutional Amendments.”⁶⁸ For Justice Goldberg, “the Ninth Amendment displayed that fundamental rights exist that are not expressly enumerated in the first eight amendments and an intent that the list of rights included there not be deemed exhaustive.”⁶⁹ This opinion arrives at a closer understanding of the fundamental right to privacy.

However, where Justice Goldberg and I differ is that the constitution contains an implicit fundamental right to privacy. The founders understood Lockean’s property argument and the

⁶⁶ Griswold v. Connecticut, 381 U.S. 479 (1965)

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Ibid.

accompanying right to privacy that followed. The founders then, in response to the disregard of their privacy by the British, explicitly stated other rights to privacy for easier understanding. These amendments are simply an extension of your personal space and property. In the same way that a receipt makes explicit that you own something, these Constitutional amendments made explicit certain privacy protections. However, even members of court do not see this as clearly. Justice Black in his dissent stated that although he likes his privacy as much as anyone, he believes that he “is compelled to admit that the government has a right to invade it unless prohibited by some specific constitutional provision.”⁷⁰ This dissent, and particularly the point regarding the right to invade, overlook that the right to privacy is grounded in the fundamental right to one’s person. There is no liberty without choice. The fourth amendment and idea of unreasonable searches does not become an established right without first understanding that one must have the ability to control one’s person.

All in all, the penumbra argument is one that is very interesting but shows a deeper lack of understanding of the right to privacy. It is not that privacy is included in the penumbra of the other rights. Instead, privacy is in the fundamental liberty granted to one’s person. The basis for the constitutional creation. “Safeguarding” in the Constitution is created from privacy, the fundamental liberty is to have the right to control something; aspects of our commitment to privacy is fundamental. The sixth amendment is making some aspects of privacy explicit and even the requirement of warrant to search and seize, all build off of our established fundamental right to privacy. So, what becomes clear is that the right to privacy is encoded in the law and extends to govern moral privacy.

⁷⁰ Griswold v. Connecticut, 381 U.S. 479 (1965)

Chapter 6: Privacy-as-property

I have now considered Locke's property rights, the constitution's implicit recognition of the right to privacy, Warren and Brandeis, and a past SCOTUS, I can now establish what the right to privacy truly is. All of these examples help led us to our answer that the right to privacy is an extension of the property right one has over one's person. The right to control yourself is inalienable and fundamental; there cannot be any terms where someone can own you without creating an egregious violation to one's right to privacy. As well, the innate right to privacy, through control of one's own person, extends to other forms of one's property, including homes, smartphones, and cloud data. In the same light the constitutional right to privacy explicitly expressed the implicit aspects of the right to privacy. Nuisance law, as seen in Warren and Brandeis, also bolsters our definition of the right to privacy. The fundamental right seen in nuisance law is sovereignty over your personal space. If someone is doing something which in turn constricts your personal space that too will undermine your right to privacy.

Privacy-as-property

1. The right to privacy begins with a property interest
2. The most fundamental property is one self's physical body and mental space
3. Every individual has a property in his own person and this right is one that nobody has a right to, but themselves
4. Thus, the right to privacy is the right to control oneself
5. The right to control oneself, naturally extends to extrinsic objects which you own. Including your data physical items or non-physical cloud storage information
6. The ability to control oneself means that you must consent to the use of yourself in any, establishing privacy protection
7. If you are not truly provided the choice to accept or deny consenting to the use your person or information, your right to privacy is violated
8. Because my right to privacy begins with my right to control myself, by "accepting" an agreement to use a third-party app I am not tactically consent, or relinquishing, my right to privacy

The most fundamental aspect of liberty is the ability to control oneself and that is manifested in the constitution. Nonetheless, this fundamental right must be reconsidered and applied with the advancement of new technology. In the past it would not be a violation of my privacy if you were simply walking across my land (property) and passing by without looking into or entering my home. If you planted a bug in my home, your eavesdropping would've violated my privacy,⁷¹ but if I was at the restaurant speaking aloud you would not be intruding my right to privacy. However, with the advancement of technology it is no longer this easy to have the distinction. The physical boundary that once safeguarded my property is now a figurative cloud where all of my data, information, and life can easily be scraped together to curate specific advertisements; or someone can be listening to every word that I say while my phone is near me. Big Tech has systematically violated the right to privacy that has been established in this paper. However, there are some individuals who are willing to consent to lose their right to privacy in order to obtain the benefits of innovation. For those willing to consent that is their choice, but it is those who have no option to consent who's right to privacy are being violated.

⁷¹ *Hamberger v. Eastman*, 106 N.H. 107, 206 A.2d 239 (N.H. 1964): a case in which tenants sued their landlord after discovering he had installed an eavesdropping device in their bedroom. - should I expand this example further?

Part 2: Technology, Tacit Consent, and Evolving Business Practices

Chapter 7: We're All Being Tracked

I want to introduce you to Aericka. She is a middle-aged woman who actively, in her opinion, avoids all social media. The reason? Well, she believes that these sites do not respect your privacy, and because everyone shares information on these sites there is ultimately no privacy on these websites. For someone who actively attempts to stay away from these sites, she must still use technology. Her work requires it, connecting with family and friends requires it, and even other elements of personal activities such as workouts, all use technology. Browsing the internet is also a daily task. The secret? That even for someone who attempts to protect themselves from forms of data sharing, she is still being tracked and sharing information to big tech companies.

In our current world sharing information is simply a necessary part of life. Much of the sharing that we do is nearly impossible to avoid if we have any desire to participate in modern life. Simply browsing the Internet is an event in which you are sharing data with the company providing that service. Purchasing anything on Amazon, setting up a phone number, utilizing online banking, paying for goods with a credit card, opening Google Maps and the list could continue indefinitely, involves significant online data disclosures.⁷² And for the billions of people who are not like Aericka, including myself, who are active on social media the sharing is multiplied ten-fold. Therefore, because this act of sharing is completed out of necessity - whether

⁷² Waldman, *Privacy as Trust*, 67-8

this includes work, gaining information, or being a social person - it cannot truly be a matter of free choice.⁷³ Because much, if not all, of our online sharing is constructively involuntary, any argument that claims we no longer have a right to privacy over our data because we “agreed to use that corporation's services” is invalid. Therefore, any claim that users have “tacitly consented” to have surrendered our right to privacy is invalid. The established framework of *privacy-as-property* protects us from these claims.

So, when Aericka’s friend sends her a link to Pinterest, she joins. After the pushback, why would she succumb to a social media site? Well, it’s simple, we as humans, “have social reasons to participate on social network sites.”⁷⁴ Did she now lose her right to privacy? Can that corporate do with her information as they please since she agreed to the “terms and conditions?” The answer is no. Do you lose your right to privacy simply because you agreed to use a telephone service provider? Can the phone company simply give all your past calls logs without reason simply because we used a service, provided by their cell towers? The answer to these questions is no.

It doesn’t really matter why we decide to use a third-party service. Many times, it’s necessary to conduct daily tasks - such as having a cell phone. Other times it’s to be a social being or to order something to your house to save you time. During the COVID-19 pandemic the latter has even become considered one of the safest ways to shop. And sometimes we “agree” to terms and conditions to simply get a 15% off reward. Sure, you might on paper have a choice to not use services. You theoretically have the choice to not provide your email address to get 15% off. The choice may simply be pay the non-discounted price. So, on paper it might seem like we have a choice, but when you truly think about your daily tasks can you conclude that we really

⁷³ Waldman, *Privacy as Trust*, 68

⁷⁴ *Ibid*, 56.

have a choice? The answer, once again, is no. Sure, I might have the choice to not “accept the mandatory cookies” when I enter a website but if I decline that option, I have no other choice than to leave. Whether or not you might feel comfortable sharing information, in the age of technology, comfort doesn’t matter:

“I know that I’m being watched online, but I don’t really know how to factor that into what I do. I mean, it’s not like I can decide not to enter in my credit card information if I need to buy something on Amazon.”⁷⁵

Therefore, the reason for why we are using, or sharing our information, with third-parties - specially tech companies - has no current bearing⁷⁶ on justifying whether or not we maintain our right to privacy. A multitude of our initial disclosures, the willingness to use a third-party service, do not result from having a perfectly free choice.⁷⁷ Instead sharing information is a necessary result of living in a world where networked technology is integrated with everything. Where our physical property is now both a physical property on earth and figuratively in a cloud.

⁷⁵ Waldman, *Privacy as Trust*, 55

⁷⁶ I will present a consideration of consenting to third parties that can allow us to actually consent. This will be through an “opt-in” option

⁷⁷ Waldman, *Privacy as Trust*, 68

Chapter 8: Tacit Consent. Smith trumps Locke.

Throughout the COVID-19 pandemic the success of technology has made many aspects of a difficult situation bearable. The ability to communicate with others instantaneously, without being face to face, has become a necessity. However, those creating the technology also have a business model that excels in scraping individual's data to create better advertisements, better products, and monetize the information they receive. Those monetary interests can at times come into clear violations to users' right to privacy. Look no further than Facebook and Cambridge Analytica scandal of 2014. In this leak Cambridge Analytica, acquired the private Facebook data of tens of millions of users — the largest known leak in Facebook history.⁷⁸ In this light we have also seen the rise of privacy leakages in the use of Alexa systems across the world. From sending full recorded conversations to contacts in your phone, to employees listening to your interactions with Alexa.⁷⁹ Apple, in the same light, was allowing private conversations with Siri to be listed by contractors.⁸⁰ The hundreds of pages of terms and conditions on social media applications, when you first turn on your phone, download a new app, may provide notice of how your data *might* be used. For the millions, maybe billions, of users that may be selecting “agree” to use the product are not consenting to forfeit their fundamental right to privacy. What is the other choice? Read the terms and conditions? The same policies that are single-spaced, written in small font

⁷⁸ Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” *New York Times*, April 4, 2018. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

⁷⁹ Jeb Su, Why Amazon Alexa Is Always Listening To Your Conversations: Analysis, *Forbes*, May 16, 2019. <https://www.forbes.com/sites/jeanbaptiste/2019/05/16/why-amazon-alexa-is-always-listening-to-your-conversations-analysis/?sh=6e1abe7e2378>

⁸⁰Jeb Su, Confirmed: Apple Caught In Siri Privacy Scandal, Let Contractors Listen To Private Voice Recordings, July, 30, 2019, <https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/?sh=48f894077314>

sizes and are often misleading,⁸¹ “confusing, inconspicuous, and inscrutable”⁸² even for legal scholars? Lorrie Faith Cranor, a computer science, engineering, and public policy scholar at Carnegie Mellon University, estimates that it would take a user an average of 244 hours per year to read the privacy policy of every website she visited.⁸³ This would amount to roughly 54 billion hours per year for every U.S. consumer to read all the privacy policies he or she encounters.⁸⁴ The other choice is to simply “accept” without reading. Did you really have a choice in the first place? Do you really have the chance to spend an extra 10 days a year reading every policy for every website you visit, app you download, or purchase you make? No, and therefore you are still protected by the *privacy-as-property* conception every time you do “accept” one of these agreements.

As I have established the right to privacy begins with the fundamental right to have control over one’s person. The right to control oneself extends to your external objections that you purchase and govern them at all times whether or not they are in your physical possession. Therefore, it is now important to consider how the conception of privacy I have established applies to your everyday data when you interact with cell phone towers, social media sites, and more on phone, tablet, Alexa, or any other device. Do we automatically forfeit - tacitly consent away - our right to privacy because we are using these new technologies and gain access to a plethora of information at our fingertips? As I have previously established, the answer is no, and the justification can be found in a further elaboration of tacit consent. Because of our

⁸¹ Lorrie Faith Cranor, “Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice,” *Journal on Telecommunication and High Technology Law* 10, (2012): 273-274
http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Cranor.PDF

⁸² Waldman, *Privacy as Trust*, 66

⁸³ Aleecia M. McDonald and Lorrie Faith Cranor, “The Cost of Reading Privacy Policies, *A Journal of Law and Policy for the Information Society*,” vol. 4, no. 3 (2008): 563. <http://hdl.handle.net/1811/72839>

⁸⁴ *Ibid.*

fundamental establishment of privacy, you cannot simply give away your right to privacy, the right to control oneself, over without explicit consent.

From the Lockean perspective, the outcome of this innovative technology is simply a by-product of our *tacit consent*. Under this perspective we as internet users would relinquish our right to privacy the moment, we accept the terms and conditions. John Locke used this perspective of tacit consent to determine the necessity of legitimate governmental rule:

By a tacit and voluntary consent, found out a way how a man may fairly possess more land than he himself can use the product off.... By putting a value on gold and silver, and tacitly aggressing in the use of money: for in government laws regulate the right of property, and the possession of land is determined by positive constitutions.⁸⁵

When applied to our modern day, because we use technology, we are tacitly consenting to giving up our right to privacy. The same government laws which regulate possession of technological devices would simply be enough to ensure laws that govern your right to privacy exist.⁸⁶ This argument may justify key violations to our fundamental right to privacy but does not make them any more convincing. This is where the Locke perspective does not help to further the establish *privacy-as-property* that I have already established. Instead, we must turn to Adam Smith for the answer regarding business neglect of the right to privacy.

Adam Smith disagrees with Locke on the topic of tacit consent. Smith, in his *Lectures on Jurisprudence*,⁸⁷ reaches the topic of “exorbitant taxation”⁸⁸ in which he discusses Locke’s consent theory; specifically, the idea of “implied consent” or tacit consent. Smith applies

⁸⁵ Locke, *Second Treatise of Government*, Sec 50.

⁸⁶ This encompasses notice and choice arguments that will be further discussed.

⁸⁷ Adam Smith, *Lectures on Jurisprudence* (1763), (ed by. R. L. Meek, D. D. Raphael, and Peter Stein) Oxford University Press: The Glasgow Edition of the Works and Correspondence of Adam Smith, Vol. 5: Lectures on Jurisprudence (1978)

⁸⁸ Smith, *Lectures on Jurisprudence*.

Locke's notion to the idea that if individuals of a state choose to not revolt (against the British government in this case) they are implying that they "consent" to the legislation of that State granted as a by-product of their citizenry in that state. Smith calls this idea, especially in terms of the exorbitant taxation, "very figurative metaphorical consent."⁸⁹ Or more specifically that there is no consent at all. Smith believes that just because individuals want to say they're legitimately taking away your consent, that doesn't mean that you've granted them your tacit consent. If you do not have a choice to conduct your actions in any way separate from the status quo, you are not tactically consenting to those laws, you're simply not consenting at all. Let's look more specifically at Smith's boat example he developed to refute Locke's account of the role of tacit consent in securing legitimate authority for the state.

The crew persons on the boat do not like the rules of the leader. From Locke's perspective by not jumping overboard, leaving the boat, they are tactically consenting to the leadership. Smith's perspective is that though the crew members are not jumping over the boat that does not mean they are tactically consenting to the leader's rules. Are these crew members truly provided a choice? A decision between jump overboard or follow the rules of leadership, doesn't seem like a choice one can make freely.

How does this example apply to our current day technology? Well consider an individual who wants to maintain their fundamental right to privacy but needs to use a phone to connect with other individuals. By the nature of cell phone terms and conditions agreements this person understands that by signing this agreement, creating a contract to use this device, their fundamental right to privacy will be violated. Nonetheless, this individual must sign the contract. Locke would consider this tacit consent but that is the wrong way to view this. We instead must

⁸⁹ Smith, *Lectures on Jurisprudence*.

apply Smith's theory to this case. We may be agreeing to terms and conditions to use a cell phone, but it has become impossible for this individual to live without a phone but by signing this agreement in no way expresses an act of consent to the violations that this individual will undergo while owning their new smart phone. To this extent, do we really relinquish all rights to our data, when we sign a contract with a cell phone provider considering the near necessity of cell phones in our current society? With our established conception of privacy and tacit consent the answer is no.

To truly uphold privacy rights, individuals must be protected from being in positions in which they are effectively forced to give up this right. You don't have the right to surrender your privacy protection if you are forced to accept terms and conditions, in order to function in society. Or forced to decide between living and following a leader you don't respect or jumping over a boat. It is the role of the courts and the legislature to protect the fundamental right to privacy, as it is to protect the right to vote or to freedom of expression.

So, without tactically consenting to the breaches, but requiring a phone, how does the government safeguard the right to privacy? We can turn to Supreme Court decisions to display how the government is applying the fundamental right to privacy, the ability to control the property in oneself, to technology.

Chapter 9: The Carpenter’s Rejection of Tacit Consent

On December 3rd, 2010, two men entered a Radioshack on East Jefferson Avenue in Detroit, Michigan. One pulled out a gun and demanded that the staff at the Radioshack fill his laundry bags with all of the newest smartphones. Their getaway driver Timothy Carpenter was waiting in a car nearby. These types of robberies continued until some of the individuals were caught. During their interrogations many of the other robbers provided information to the authorities in hopes of plea deals. One piece of evidence included Timothy Carpenter's phone number. This information was extremely vital to the investigating officers. With this number the authorities were able to serve a court order, known as a d-order from the 1980 Stored Communications act, to Carpenter's cell phone company, MetroPCS.⁹⁰ Under those current laws there was no requirement to obtain a warrant prior to requesting the data. Within days MetroPCS turned over 127 days of cell-site location data for Carpenter.⁹¹ The data was so vast, that its accuracy showed that Carpenter had been at the scene of the crime. However, the question then asked as this case made its way to the supreme court was “Does the warrantless search and seizure of cell phone records, which include the location and movements of cell phone users, violate the Fourth Amendment?”⁹² However, I believe that at the heart of this, is whether or not Carpenter tactically consented to give up his right to privacy when he signed his phone contract. The rule that encapsulates this concept is known as the third-party doctrine.

In the Oral argument Justice Kennedy asked Carpenter’s attorney, Nathan Freed Wessler, “What is the rule that you want us to adopt in this case assuming that we keep [United States v.]

⁹⁰ Cyrus Farivar, *Habeas Data: Privacy vs The Rise of Surveillance Tech.* (Brooklyn: Melville House, 2018), xii

⁹¹ Ibid.

⁹² *Carpenter v. United States*, 585 U.S. ____ (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Miller and *Smith v. Maryland* on the books. Justice Kennedy in this comment was referring to the two key SCOTUS cases that established the precedent for the third-party doctrine. The concept of the third-party doctrine is that “individuals relinquish their reasonable expectation of privacy when they transact via a third party like a phone company.”⁹³

Even though *Smith v. Maryland*⁹⁴ was precedent at the time of this hearing, dissenting Justices saw the vast violation to privacy this ruling would create. Justice Powell, in his dissent, argued that government law enforcement should not have the ability to access the telephone numbers we dial without a warrant.⁹⁵ This is because, although one number may not reveal much about us, a list of numbers “could [naturally] reveal the identities of persons and the places called, and thus reveal the most intimate details of a person’s life.”⁹⁶ This worry was then codified in the law in the case of *United States v. Jones (2012)*.⁹⁷ This case, which considered the role of GPS tracking in understanding fourth amendment violations, was decided unanimously. The Court held, in line with Powell’s prior dissent, that the reason GPS surveillance, over a period of time, constituted a search was because the ability to aggregate that data reveals key insight into one’s behavior.⁹⁸ Justice Sotomayor made it explicit that the ability for police to utilize a GPS device to track a car on public roads, would still necessitate the need for a search warrant. The ability for one to aggregate and analyze all of your data - in this case GPS locations - is a profound violation of one’s fundamental right to privacy.

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public

⁹³ Farivar, *Habeas Data: Privacy vs The Rise of Surveillance Tech*, xii.

⁹⁴ *Smith v. Maryland*, 442 U.S. 735 (1979), <https://supreme.justia.com/cases/federal/us/442/735/>

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*

⁹⁷ *United States v. Jones*, 565 U.S. 400 (2012), <https://www.supremecourt.gov/opinions/111pdf/10-1259.pdf>

⁹⁸ *United States v. Jones*, 565 U.S. 400, 413–18 (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring in the judgment)

movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on... The unique attributes of GPS monitoring” – in particular, its allowance of nonstop and precise surveillance – implicates the Fourth Amendment’s guarantee against unreasonable searches and seizure:⁹⁹

The Supreme Court ultimately decided in the *Carpenter* that the government must obtain a search warrant in order to request the cell phone records from a phone company.¹⁰⁰ The majority opinion written by Chief Justice Roberts displays the courts understanding of the fundamental right to privacy. Justice Roberts wrote, in a 5-4 decision, that the historical privacy of cell site location information required a “legitimate expectation of privacy in the record of his physical movements.”¹⁰¹ This was because the method of tracking cellular location data will provide a “near-perfect surveillance”¹⁰² into the lives of individuals. Allowing government access to cell-site records—which “hold for many Americans the ‘privacies of life,’ ” *Riley v. California*, 573 U. S. ___, ___—contravenes that expectation.¹⁰³ Roberts detailed that even though there is no physical invasion of privacy, by viewing electronic records and data, they pose the same - if not a greater - invasion of individual privacy. This information grants the ability for the government to access intimate details of one’s life, and constitutes a search. The lawyers arguing for the United States government put forth an argument that there was, in effect, tacit consent by *Carpenter* to release his cell phone information because of his signed contract. However, the majority opinion Justice Roberts determined the opposite. Roberts stated that simply because the United States has laws governing third parties, in this case cell phone

⁹⁹ *United States v. Jones*, 565 U.S. 400, 413–18 (Sotomayor, J., concurring)

¹⁰⁰ *Carpenter v. United States*, 585 U.S. ___ (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

¹⁰¹ *Ibid.*

¹⁰² *Ibid.*

¹⁰³ *Ibid.*

companies that possess citizens data, it does not mean that individuals no longer have Fourth Amendment protection regarding information disclosed to a company.

Thus, it is important to recognize here that my established account of the right to privacy, including Smith's account of tacit consent, both explains and justifies the Court's reasoning in this case. One does not forfeit their right to privacy, or tactically consent to the use of their private data, simply because they are forced to sign a contract with a telephone provider to use a cellphone. See the Court had already created a precedent in their unanimous decision of *Riley v California* (2014)¹⁰⁴ that the warrantless search exception following an arrest exists for the purposes of protecting officer safety and preserving evidence, neither of which is at issue in the search of digital data.¹⁰⁵ Justice Roberts wrote in the majority opinion that digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape.¹⁰⁶ Therefore, one can search the phone to ensure that it wouldn't be used as a weapon, to see if has a knife attached to it, but one cannot search the contents of the phone.¹⁰⁷ More importantly to our discussion on the fundamental right to privacy, is that the Court also held that information accessible via the phone but stored using "cloud computing" is not even "on the arrestee's person."¹⁰⁸ This means that the *privacy-as-property* explains the true reasoning for how this decision can be quantified in the law. The conception of privacy, that you have the ability to control oneself, and that property interest in oneself extends to external possessions, has been recognized to include both physical objects and cloud data. What is the importance of

¹⁰⁴ See also: *Weeks v. United States*, 232 U.S. 383 (1914), <https://supreme.justia.com/cases/federal/us/232/383/>; *Chimel v. California*, 395 U.S. 752 (1969), <https://supreme.justia.com/cases/federal/us/395/752/>; *Wyoming v. Houghton*, 526 U.S. 295 (1999), <https://supreme.justia.com/cases/federal/us/526/295/>

¹⁰⁵ *Riley v. California*, 573 U.S. 373 (2014), https://www.supremecourt.gov/opinions/13pdf/13-132_819c.pdf

¹⁰⁶ Although, the Court held that some warrantless searches of cell phones might be permitted in an emergency: when the government's interests are so compelling that a search would be reasonable.

¹⁰⁷ *Riley v. California*, 573 U.S. 373 (2014), https://www.supremecourt.gov/opinions/13pdf/13-132_819c.pdf

¹⁰⁸ *Ibid.*

Carpenter and Riley? It is the articulation by the Court, of that the right to privacy is a fundamental right.

In *Carpenter*, the Court made explicit what was already implicit in the constitution; the right to privacy is derived from the property right in oneself. The cell phone data that is stored on the phone, even though you are paying a phone company to use the service, is still your private information. This information is your private property which is protected by the Fourth amendment. What is the common denominator between your cell phone data and your person? It is that in the current day, your cell phone is a key extension of your person. In developed countries it is extremely difficult to be able to live daily life without a cell phone. Therefore, this digital data that is stored is simply another example of you being in your home. The intrinsic right to property over oneself is extended to their external items they purchase. They have effectively mixed their labor with these products. Simply put, because a your property may be extrinsic instead of intrinsic (to one's body) it does not alter the privacy protection that is endowed unto it. That is exactly what the *stare decisis* in *Riley v. California* established and was extrapolated to apply in the *Carpenter* case.

This case is crucial to understanding the fundamental right to privacy. The Courts have made it explicit that personal information that is not on one's person, is still protected against unreasonable search and seizures. The aforementioned protection against unconstitutional searches (Fourth Amendment) derives from the implicit understanding in the Constitution that the fundamental right to privacy starts with a property right in oneself. It is the role of the courts and the legislature to protect the fundamental right to privacy, as it is to protect the right to vote or to freedom of expression. *Carpenter* best explains the effort by the Supreme Court to protect this right to privacy when applied to cell phone records.

The government's use of data aggregation, without first obtaining a warrant, was established as a violation to the right to privacy, namely the Fourth Amendment. How does this then relate to the aggregation of our information by tech companies? What protection to the right to privacy is offered in this area?

Chapter 10: Data Aggregation: What Permits This?

Government use of data aggregation is a violation of our right to privacy and the same must be said for companies that do the aggregate our cloud data. Taken at face value visiting one website or bringing your phone with you to the store is not a violation of your privacy. That website gains information that you visited it and your GPS might put you at the store. However, when that GPS then communicates with that website, and all other websites you visit this now provides a multitude of intimate data that can explain, among other things, who you are, what you do, and where you go. When analyzed together, they reveal intimate information into your very personal life. Therefore, aggregated data serves a greater purpose than simply being the “sum of its parts.”¹⁰⁹ This data can be used, and analyzed, to improve advertising, decision making, and predictive analysis. To know what you need and when you need it. To elaborate this point further we can look at a story involving Target, a pregnant woman, and an unknowing grandfather to be.

About a year after Pole created [a] pregnancy-prediction model [2003], a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, according to an employee who participated in the conversation. “My daughter got this in the mail!” he said. “She’s still in high school, and you’re sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?” The manager didn’t have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man’s daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again. On the phone, though, the father was somewhat abashed. “I had a talk with my daughter,” he said. “It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August. I owe you an apology.”¹¹⁰

¹⁰⁹ Howard Beales, “The Value of Behavioral Targeting,” *Networking Advertising Initiative*, (2010): 1-24, www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

¹¹⁰ Charles Duhigg, “How Companies Learn Your Secrets,” *New York Times*, February 16, 2012, www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

If you asked a group of individuals if this a violation of our right to privacy a majority of them would agree with this claim.¹¹¹ However, whether you agree or disagree it is clear under the conception of *privacy-as-property* that this violates our innate right to privacy. The young woman, in this example, was pregnant but had not yet told her father, but the goal of Target was to discover, using a host of data, who was pregnant before they may be willing to share that news with Target or in this case their father. The Target pregnancy-prediction model utilized an algorithm to scrape, and aggregate data. Aggregating information such as “customer shopping habits, Facebook likes, marital status, estimated salary, credit card usage, web browsing history, and much more.”¹¹² Eventually resulting in specific names of customers, which would subsequently allow Target to send them coupons.¹¹³ This specific tactic is not unique to Target. The norm of retailers, tech companies, and the growth of online advertising, attempts to use past browsing history, shopping habits, and other data, to curate specifically targeted ads. So, my search for a new apartment results in a multitude of advertisements across all social media sites for apartment complexes.

Can I choose to not have these companies track me? Well, you can certainly try, it will just involve you “periodically, cleaning your cookies, purging your Google ad history, and resetting your advertising ID.”¹¹⁴ You can use a private browser such as Firefox Focus, DuckDuckGo and Ghostery Privacy Browser, but they may inhibit your daily workflow as their features may prevent integrated parts of websites to perform their tasks correctly. You can also

¹¹¹ Lee Raine and Maeve Duggan, “Privacy and Information Sharing,” *Pew Research Center* (2016): 1-46, www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

¹¹² Duhigg, “How Companies Learn Your Secrets.”

¹¹³ Ibid.

¹¹⁴ Brian X. Chen, “Are Targeted Ads Stalking You? Here’s How to Make Them Stop,” *New York Times*, August 15, 2018, <https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html>.

“opt out”¹¹⁵ of being included in interest-based advertising, but as Facebook details “if you turn off this setting, the ads you see may still be based on your activity on our platform [and] they may also be based on information from a specific business that has shared a list of individuals or devices with us, if we've matched your profile to information on that list.” If it wasn't clear before, it now becomes extremely clear as to why we are not tacitly consenting to forego our *privacy-as-property* right when “agreeing” to terms and conditions. It becomes clear that in theory, one would have control of what data companies they can allow corporations, but in practicality it is temporary, tedious, confusing, and ultimately non-existent.¹¹⁶

The creator of Target's pregnancy-prediction model, one that aimed at discovering women who were in their second trimester, said in regard to his model that: “we [Target] are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy.”¹¹⁷ This is the issue with current laws. They do not protect users right to privacy. They allow data aggregation and create notice-and-choice policies that do not protect our fundamental right to privacy.

Notice-and-choice is a formulation of laws created by the Federal Trade Commission that focuses on corporations notifying consumers of their business, data, and privacy policies.¹¹⁸ In short, these notice-and-choice laws are an explicit version of Locke's tacit consent argument

¹¹⁵ “Control the Ads You See,” Facebook 2021.

https://www.facebook.com/help/1075880512458213/?helpref=hc_fnav. ; “Control personalized ads on the App Store, Apple News, and Stocks,” Apple, Published Date: January 7, 2021, <https://support.apple.com/en-us/HT202074>. ; “Your privacy controls for personalized ads,” Twitter, <https://help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads> ; “Block certain ads,” Google <https://support.google.com/ads/answer/2662922?hl=en>

¹¹⁶ Vindu Goel, “Flipping the Switches on Facebook's Privacy Controls,” *New York Times*, January. 29, 2014, <https://www.nytimes.com/2014/01/30/technology/personaltech/on-facebook-deciding-who-knows-youre-a-dog.html>.

¹¹⁷ Duhigg, “How Companies Learn Your Secrets.”

¹¹⁸ U.S Department of Health, Education. & Welfare, “Records, Computers, and the Rights of Citizens,” (1973): i-346, Library Department of Justice, www.justice.gov/opcl/docs/rec-com-rights.pdf: Notice-and-choice was created from the Fair Information Practices Principles (FIPPs). FIPP was established in this 1973 report from the federal Department of Housing, Education, and Welfare.

when applied to the technology age. The argument that can be formulated from notice-and-choice laws is the same one that the US government attorney articulated in *Carpenter*. If corporations are disclosing their business practices, then we all have the necessary information to consent to relinquish our right to privacy when operating with these third parties. Moreover, this legal conception is why certain individuals believe that because we “agree” to the terms and conditions written out, we no longer have a right to privacy over that information.¹¹⁹ This provides the basis for websites being able to legally aggregate our data to advance their profit-maximizing business model. Under a notice-and-choice model, the infamous 1993 New Yorker cartoon, “On the Internet, nobody knows you’re a dog”¹²⁰ would be impossible. The same way Target knew to send a pregnant woman coupons, means that a dog-surfing the internet would undoubtedly receive targeted dog food and toys advertisements.

Therefore, this current notice-and-choice law, or other conceptions of privacy, that advance a Lockean formulation of tacit consent are simply violations to the fundamental right to privacy under *privacy-as-property*. It is impossible to consent to our data being aggregated, sold or shared if we “never had the choice in the first place.”¹²¹ If you did believe Locke’s argument of tacit consent, consider the fact that even if these corporations are disclosing in these terms and agreements that they’ll use your data, what isn’t included in these disclosures are the curated algorithmic processes used to track each individual. That information is their competitive advantage over other firms, and one they don’t disclose. The algorithms are both “guarded or protected by the law of trade secrets.”¹²² Do you read the 175-page *Search Quality Rater*

¹¹⁹ M. Ryan Calo, “Against Notice Skepticism in Privacy (and Elsewhere),” *NOTRE DAME L. REV.* 87, No.3. (2012): 1027, 1049, <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/>

¹²⁰ Peter Steiner, “Cartoon: On the Internet, Nobody Knows You’re a Dog,” *New Yorker*, July 5, 1993.

¹²¹ *Smith v. Maryland*, 442 U.S. 735, 749 (Marshall, J., dissenting) (1979).

¹²² Waldman, *Privacy as Trust*, 84-85

Guidelines by Google to determine if they're using your information in accordance with your right to privacy claims? These current business practices constitute a moral, not legal, violation to our right to privacy.

This claim is in no way detailing that this business practice should be outlawed. I am not arguing for this practice, but instead for a change to the process. A shift in the codification of privacy in the law. The current opt-out policies perpetuate a violation of our right to privacy; an opt-in model, for those who have no qualms to having their data aggregated, is necessary. The legal changes to these practices will undoubtedly change in the future. Antitrust investigations are the focal point for a change in privacy laws. This will lead the laws regulating privacy to change and arrive at my conception of the right to privacy, one that aligns with *privacy-as-property*. Because consumers are not truly provided a choice to not share information, our data must be vehemently protected.

However, government processes are slow, political, and at times filled with red tape. The true change will not be led by the government, but instead by corporations. The same ones using these tactics will have to change the way they operate. The inevitably legal changes pose an opportunity for corporations to alter their practices before regulations force them to. Corporations that focus on privacy will have the opportunity to corrode the market share of corporations who do not protect the right to privacy. Before discussing the change in business practices, we must answer a few questions: Are corporations entitled to this same *privacy-as-property* protection? If not, can we require the disclosure of their algorithmic processes? Or can we mandate these corporations to have an information fiduciary responsibility?

Chapter 11: Why Businesses Are Not Entitled to Privacy-as-property

The fundamental right to privacy, *privacy-as-property*, is an individual right and is one not afforded to corporations. Take for example the case *Federal Communications Commission v. AT&T Inc.*¹²³ This case held that corporations are unable to rely on “personal privacy” to prevent FOIA disclosures.¹²⁴ This is because corporations are not natural constitutional persons, with the full range of rights recognized for such persons. They are instead carefully circumscribed artificial legal persons, with certain legislated rights that allow them to act as such circumscribed persons. An LLC is a limited liability company, a legally created entity. We can therefore demand publication of information because we cannot violate a corporation's right to privacy.¹²⁵ The only rights to privacy these corporations have are the ones that are given to them by the laws that the State which governs them creations.

This includes for example the right to contract with individuals who become employees of the corporation. Apple is one company that is very well known for their commitment to secrecy when discussing new products and features. In its new hire onboarding process, Apple requires "employees sign long, overlapping nondisclosure agreements (NDAs) and agree to abide by the company's well-known lock-down and secrecy practices."¹²⁶ Back in 2017 an Apple engineer was fired because his daughter, after spending a day with him at the Apple campus,

¹²³ *Federal Communications Commission v. AT&T Inc.*, 562 U.S. 397 (2011)

¹²⁴ *Ibid.*

¹²⁵ This, of course, does not include a discussion of patent laws. However, patent laws are legal prescribed methods to prevent others from infringing on your intellectual property. Individuals and corporations can both obtain patents. However, these laws align with the listed description of corporations as persons that are entitled to privacy protections and patents when disclosed to government entities to review and accept. The main point here is that they require disclosure mandates, where as a person does not present these same requirements.

¹²⁶ Jay Yarow, “What It’s Like on Day One as an Apple Employee,” *Business Insider*, January 26, 2012, www.businessinsider.com/what-its-like-on-day-one-as-an-apple-employee-2012-1.

released a vlog on YouTube that included a new iOS feature.¹²⁷ Apple can contract freely with their employers to ensure the enforceability of NDA but as a company they are not provided the same individual right to privacy. As a corporation they are required to present disclosures to their shareholders, regulators, and other government entities.

Another example of this is the case of *Citizens United V. Federal Election Commission*. The Court established that corporations were allowed to exercise their first amendment right and were able to freely spend money on political speech. However, nowhere in this ruling, or elsewhere has there been a legal precedent established that corporations are people.¹²⁸ So although corporations are provided with some rights, they are not provided with the, *privacy-as-property* or the fundamental right to privacy implicit in the Constitution. Instead, they must ensure the right to privacy for individuals is upheld. If they don't willingly do this, competition and laws will force them to.¹²⁹

My conception of the right to privacy, *privacy-as-property* is one that can span intercontinental legal jurisdictions. This fundamental approach means that no matter where you are, you have the right to control yourself, and this property interest in oneself extends to your external objects you own, including your data. The ability for this approach to privacy to govern many countries makes privacy an integral part of liberty for all. Despite the focus of this paper revolving around the aggregation and data violations focused primarily on the United States, *privacy-as-property* must be established in all countries. However, when it comes to data

¹²⁷Zara Stone, "Daughter Of Fired iPhone X Apple Engineer Is Really, Really Sorry," *Forbes*, October, 31, 2017, <https://www.forbes.com/sites/zarastone/2017/10/31/daughter-of-fired-iphone-x-apple-engineer-is-really-really-sorry/?sh=446cf169ad76>.

¹²⁸ *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), <https://www.supremecourt.gov/opinions/09pdf/08-205.pdf>

¹²⁹ Adam Satariano, "Europe Proposes Strict Rules for Artificial Intelligence," *New York Times*, April 21, 2021, <https://www.nytimes.com/2021/04/16/business/artificial-intelligence-regulation.html>.

protection issues, the Atlantic Ocean represents a rift between the Europe Union and the United States.

Europeans have much more bureaucratic data protection laws.¹³⁰ Article 25 of the European Data Protection Directive states that personal data may only be transferred to “third countries that ensure an adequate level of data protection, i.e., a level equivalent to the protection in the European Union.”¹³¹ However, after contentious legal battles between the United States and the EU, the Safe Harbor Agreement was created. Accordingly, US-companies can commit themselves to follow the Safe Harbor Principles and register themselves in a list of the US Department of Commerce. This will allow companies to be treated as appropriate recipients for the transmission of data.¹³² This provides a practical and legally acceptable solution for the data transmission between Europe and the United States.¹³³ Therefore, with our established right to privacy, all countries should - and can - implement the same rights and data protection to their citizens due to the *privacy-as-property* approach right to privacy. Germany’s data protection doctrine includes this conception: “the collection, processing and use of personal data shall be admissible only if permitted or prescribed by Act or any other legal provision or if the data subject has consented.”¹³⁴

The further advancement of AI will undoubtedly alter the landscape of the world. This powerful technology can lead to fully autonomous vehicles, robots, and endless other

¹³⁰ Dieter Dörr, and Russell L. Weaver. *The Right to Privacy in the Light of Media Convergence – : Perspectives From Three Continents (Media Convergence / Medienkonvergenz)*. Berlin: De Gruyter, 2012), 357
<http://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=nlebk&AN=471029&site=ehost-live&scope=site>. 357-8.

¹³¹ *Ibid.*

¹³² *Ibid.*

¹³³ *Ibid.*

¹³⁴ Farivar, *Habeas Data: Privacy vs The Rise of Surveillance Tech*, xiv

possibilities. Artificial intelligence is already utilized in call centers,¹³⁵ by law enforcement, in determining credit scores and bank lending,¹³⁶ hiring decisions, exam scoring, and electronic assistants. Ultimately the wide-ranging use of artificial intelligence can easily lead to violations of the right to privacy. It can involve discriminatory legal practices, advertisement, and scraping, the process of instantaneously aggregating your data. Globally, these violations to privacy are no longer being taken lightly. Countries like Canada, the United States, Australia are enacting policies to prevent the further eroding of our right to privacy,¹³⁷ with Europe leading legislative reform. The European Union has proposed the first policy in the world governing the use of artificial intelligence (AI).¹³⁸ The same technology that helps to achieve the aforementioned examples of data aggregation. This *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*¹³⁹ establishes key disclosure agreements for corporations. If enacted, this policy would require human oversight in the use and creation of artificial intelligence. It would also mandate that “companies providing artificial intelligence in high-risk areas provide regulators with proof of its safety, including risk assessments and documentation explaining how the technology is making decisions.”¹⁴⁰

However, the key to true advancement in privacy law is for these countries to instill a consistent approach to regulation. My conception of *privacy-as-property* and the inability for individuals to tactically consent away their data, provides that foundation. The codifying of

¹³⁵ Kevin Roose, “A Machine May Not Take you Job, but one could become your boss,” *New York Times*, June 23, 2019, <https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html>.

¹³⁶ Satariano, “Europe Proposes Strict Rules for Artificial Intelligence

¹³⁷ Paul Mozur, Cecilia Kang, Adam Satariano and David McCabe, “A Global Tipping Point for Reining In Tech Has Arrived,” *New York Times*, April 20, 2021, <https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html>.

¹³⁸ Satariano, “Europe Proposes Strict Rules for Artificial Intelligence.”

¹³⁹ “Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),” European Commission, last update April 26, 2021, <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence>

¹⁴⁰ Satariano, “Europe Proposes Strict Rules for Artificial Intelligence.”

privacy in the law is necessary and forthcoming. Corporations must change their business practices to reflect *privacy-as-property* before it's too late.

Chapter 12: Apple's Launch into *Privacy-as-Property*?

When it comes to technology and the right to privacy, the current business model of forcing users to agree to the documents is perpetuated by the notice-and-choice doctrine. These laws are insufficient in truly protecting the privacy of individuals. Global laws will eventually regulate practices in a way that aligns with my conception of the right to privacy. It will be necessary to codify the right to control oneself is central in the technology age. General Data Protection Regulation (GDPR) in the European Union is another example of ensuring that consumers have full control over their data. It reinforces that we have a property right in oneself and there can control the dissemination of data.¹⁴¹ Canada has enacted the The Personal Information Protection and Electronic Documents Act (PIPEDA) to ensure that “personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, they must obtain consent again.”¹⁴² The Privacy Act then controls how the federal government's ability to “collects, uses and discloses your personal information.”¹⁴³

As I have previously established there are theoretically ways to protect your privacy in this age of being forced to agree to terms and conditions, cookies, and contracts that span hundreds of pages.¹⁴⁴ However, these actions are temporary, tedious, and impractical. Current laws regulation business practices are simply backwards when compared to my established fundamental right to privacy. They allow for a notice-and-choice conception to prevail in the

¹⁴¹ General Data Protection Regulation, Regulation (EU) 2016/679, OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, *Intersoft Consulting*, <https://gdpr-info.eu/>.

¹⁴² “PIPEDA in brief,” Office of the Privacy Commissioner of Canada, Revised May 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

¹⁴³ “The Privacy Act in brief,” Office of the Privacy Commissioner of Canada, August 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

¹⁴⁴ See Chapter 10

law. The right to privacy in law, after understanding *privacy-as-property*, is fairly straightforward. Since individuals have a property interest in controlling themselves, the default for privacy and the way it must be codified in the law, is that consumers must *opt-in* to allow their data to be aggregated. It is the role of the courts and the legislature to protect the fundamental right to privacy. To truly protect the right to privacy, individuals must be protected from being in positions in which they are forced to give up this right.

Current laws don't give you a choice as to whether or not you have the right to surrender your privacy protection. You are simply forced to accept terms and conditions, in order to function in society. Therefore, with a fully opt-in system you can *consent* to forego your right to privacy to have the full convenience of the innovation. This method would truly allow each consumer to have a choice. Each individuals' right to privacy would be upheld while also allowing willing individuals the ability to trade their right to privacy in order to obtain additional benefits of technology. Thus, upholding your inherent right to your own person. The law will eventually reach this conclusion, the United States Supreme Court has already established a foundation for privacy to be codified in the law as a property interest in oneself. In the meantime, there represents a market prime for capitalization. The market share for corporations that truly uphold the right to privacy will alter business practices. Consumer trust and confidence in privacy protection will undoubtedly increase revenue in the future. Corporations already understand the importance of privacy. This is why when an Apple user attempts to load iCloud on a new device, Apple prompts a pop up asking if they "Trust this Computer or Trust this browser." Then requiring approval via your main device or a 6-digit code to gain access to your data. Google automatically alerts you if you sign in via a new device and will ask you to establish a trusted device to enter one of three numbers prior to signing in. Passwords even serve

as a form of property protection; this can be analogous to building a fence around your house in, it allows you to control who comes in and out. Businesses far and wide understand the importance of privacy, the importance of ensuring that the individual, the owner of that data, has the right to control, sign into their device. Snapchat’s growth to popularity came from a seemingly trivial concept, that after you send something it disappears. But the selling point behind it was an inherent conception of privacy. Consenting to what you send and how long you want it to be viewed for. Other corporations have followed this path including Instagram stories. But on the other hand, the profit-maximizing methods of data aggregation have blinded the desire to uphold the right to privacy. Snapchat was found to keep in their system these photos and messages there we supposed to disappear¹⁴⁵ and Facebook was fined five billion dollars over privacy violations.¹⁴⁶

However, corporations will no longer have this choice of maximizing profit over privacy. The businesses that don’t adjust to protecting the right to privacy, before the law enacts the *property-as-privacy* conception, will cede market share to other competitors in the industry. This is why we have seen changing business models – an emphasis on greater privacy - from corporations like Apple¹⁴⁷ and Google.¹⁴⁸ Apple is leading the “Big Tech” change with their new App Tracking Transparency iOS 14.5 update. This change is three-fold. On one hand it displays the recognition by technology companies, that have benefited from moral violations of privacy,

¹⁴⁵ In re Snapchat, Inc., FTC File No. 132 3078, No. C- 4501 (F.T.C. May 8, 2014), www.ftc.gov/system/files/documents/cases/14_0508snapchatcmpt.pdf (alleging that Snapchat did not fulfill many of its privacy promises, including image deletion).

¹⁴⁶“FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook,” Federal Trade Commission, July 24, 2019, <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

¹⁴⁷“Data Privacy Day at Apple: Improving transparency and empowering users,” Apple, January, 27, 2021, <https://nr.apple.com/dE5w5d0n8O>

¹⁴⁸Megan Graham, “Google says it won’t use new ways of tracking you as it phases out browser cookies for ads,” March 3, 2021, *CNBC*, <https://www.cnbc.com/2021/03/03/google-says-it-wont-track-you-directly-in-the-future-as-it-phases-out-cookies.html>.

of the fundamental right to privacy. The second is a necessity to help increase consumer trust in their products. Thus, increasing consumer demand for their product, before government regulations force change. Lastly, one of the largest proponents of this change can be attributed to the surging popularity of privacy first applications like the non-profit messaging app Signal. Due to Signal being a non-profit¹⁴⁹ their business model is vastly different when compared to the large corporations. For this non-profit entity, there is no advantage to disregarding the fundamental right to privacy but instead they gain respect, viability, and market share by robustly respecting this right.

Signal does what the laws lack. As discussed, businesses are not required to disclose the algorithmic technology they use for data aggregation. Signal Messenger willingly discloses their technology.¹⁵⁰ Signal places privacy at the forefront of their end-to-end encryption, that doesn't allow Signal itself, or any other corporations, to track you text conversations.¹⁵¹ There are no ads, affiliate marketers or external tracking within Signal messenger. It is also a free to use app, just like WhatsApp or Facebook Messenger, but with an emphasis on privacy protection. The truth is that Signal's business model is "the most scalable encryption tool we have."¹⁵² It is a fully transparent, privacy protected, way to stay connected and unlike the other privacy browsers we described, you are not limited in any way. For Signal, privacy protection isn't optional, there is no way to opt in or opt out, it's simply the default mode. So when Apple announced the App Tracking Transparency feature, and WhatsApp responded by informing users it will share data

¹⁴⁹ Signal Foundation, <https://signalfoundation.org/>

¹⁵⁰ Ibid.

¹⁵¹ Signal (App), <https://www.signal.org/>

¹⁵² Ibid. Quote by Laura Poitras

with parent company Facebook,¹⁵³ users flocked to Signal.¹⁵⁴ With roughly 7.5 million new users added that week.¹⁵⁵ What is evident regarding the exodus of users from other platforms to Signal, is that users are beginning to think more about their privacy. Some proponents of my rejection of the tacit consent argument may say that this is good enough. They may say “if I didn’t like WhatsApp then I have the choice to use an ephemeral messaging application like Signal.” But my response is that this is not enough. It’s not enough of a protection of your fundamental right to privacy when we have a few applications that although are gaining in popularity, are in mass use yet. Subsequently, Signal only has one privacy setting with no option to opt in to being tracked. See there may very well be users that appreciate the convenience that data aggregation may bring. If they were searching for a new computer, an advertisement of a new great deal appears while scrolling on Instagram, that may be preferred by them. Ultimately, consumers must have this choice.

The surge in popularity of Signal, apps like it, and the shifting focus of consumers on the right to privacy, will force corporations to adopt their policies. The approach must come from the top down starting with the big tech companies, it must include an opt-in feature for those who want the added convenience data aggregation can entail. Apple, although they have touted privacy of their devices of the years, has now taken this approach. In June 2020, Apple announced at their annual Worldwide Developers Conference that iOS, the software that powers their iPhones, would include a new privacy feature.¹⁵⁶ The Identifier for Advertisers (IDFA) that

¹⁵³Carly Page, “WhatsApp Delays Privacy Changes Amid ‘Confusion’ About Facebook Data-Sharing,” *Forbes*, January 15, 2021, <https://www.forbes.com/sites/carlypage/2021/01/15/whatsapp-delays-privacy-changes-amid-confusion-about-facebook-data-sharing/?sh=16a114674dbc>

¹⁵⁴ David Curry “Signal Revenue & Usage Statistics (2021),” *Business of Apps*, March 10, 2021, <https://www.businessofapps.com/data/signal-statistics/>

¹⁵⁵ Clare Duffy, “Why messaging app Signal is surging in popularity right now,” *CNN Business*, January 13, 2021, <https://edition.cnn.com/2021/01/12/tech/signal-growth-whatsapp-confusion/index.html>.

¹⁵⁶ “WWDC 2020 Special Event Keynote — Apple,” Apple, YouTube, 55:14 – 1:03:32, June 22, 2020, <https://youtu.be/GEZhd3J89ZE>

was utilized as an identifier in iOS for many years allowed advertisers to track your usage across multiple apps and browsers. This IDFA was automatically turned on for iPhone users but that will no longer be the case.

We believe that tracking should always be transparent and under your control. So moving forward app store policy will require Apps to ask before tracking you across apps and websites owned by other countries...we'll require developers to self report their practices. You can see if the developer is collecting a little bit of data on you or a lot of data, or if they're sharing data with other companies to track you, and much more. So for each app, you can see highlights of their privacy information before you download it.¹⁵⁷

Ultimately, this new Apple iOS App Tracking Transparency,¹⁵⁸ in the words of Craig Federighi Apple's Senior Vice President of Software Engineering, “gives users the choice of whether they wanna be tracked across apps and websites.”¹⁵⁹ Does this sound familiar? Of course it does. *Privacy-as-property* begins with the ability to control oneself. If one does not have the choice to choose how they share their information, they do not have the ability to control themselves. This is exactly how Federighi articulates his frustration with pop-ups on websites: “I share your frustration with sometimes being bombarded with every website usually telling you that they’re going to track you with a big blue accept button and no real choice at all.”¹⁶⁰ Even though Craig never used the words tacit consent while describing these examples, it is a clearly articulated rejection of past practices that don’t provide individuals any choice. This supports my rejection of any Lockean based tacit consent argument that states individuals relinquish their right to privacy by agreeing to terms and conditions.

¹⁵⁷ “WWDC 2020 Special Event Keynote — Apple.”

¹⁵⁸ Apple Developer, “App Tracking Transparency,” Apple 2021, <https://developer.apple.com/documentation/apptrackingtransparency>

¹⁵⁹ “Apple’s Craig Federighi Explains iOS 14.5’s Privacy Features | WSJ,” Wall Street Journal, YouTube, 8:05, April 26, 2021, <https://youtu.be/G05nEgsXgoI>

¹⁶⁰ Ibid.

Those who stand by the Lockean conception of tacit consent may turn to notice-and-choice laws. So, what did Apple say in regard to notice-and-choice? They may not have explicitly mentioned notice-and-choice laws, but it is Apple's goal to ensure each user has a clear understanding of what they're making a decision about and how that developer will use that data if they opt-in.¹⁶¹ Apple is clearly displaying that notice-and-choice laws are simply not enough to protect the right to privacy. They don't provide consumers a choice because it does not articulate information in a simple and concise manner for consumers. Apple made it evident that they are expanding the privacy conception of their business to effect change on a larger scale. Emphasizing their belief that "privacy is a fundamental human right."¹⁶²

It is important to recognize here that my established account of the right to privacy, including Smith's account of tacit consent, both explains and justifies Apple's reasoning for this new privacy feature. In addition, the most important aspect of this new feature is that it provides users with a choice. For those who want to allow apps to track them they can select that feature. For individuals who prefer to not be tracked, this will allow them to select that option. The fundamental right to privacy requires the ability to control oneself. This requires the ability to make free choices. One does not have this right if they are forced, in order function in society, to give up that right. *Privacy-as-property* requires these elements to achieve the right to privacy and this is what Apple is upholding with this new policy.

¹⁶¹ "WWDC 2020 Special Event Keynote — Apple," Apple, YouTube, 55:14 – 1:03:32, June 22, 2020, <https://youtu.be/GEZhD3J89ZE>

¹⁶² Ibid.

1. The right to privacy begins with a property interest
 - a. Apple: Our product work is grounded in a set of privacy principles
2. The most fundamental property is one self's physical body and mental space
 - a. Apple: "Our devices contain our most sensitive information"
3. Every individual has a property in his own person and this right is one that nobody has a right to, but themselves
 - a. Apple: Users must have the choice
4. Thus, the right to privacy is the right to control oneself
 - a. Apple: iOS 14.5 ATT: "Allow" or "Ask app not to track"
5. The right to control oneself, naturally extends to extrinsic objects which you own. Including your data physical items or non-physical cloud storage information
 - a. Apple: One should have the ability to choose whether or not they want to be tracked across apps
6. The ability to control oneself means that you must consent to the use of yourself in any, establishing privacy protection
 - a. Apple: "I share your frustration with sometimes being bombarded with every website usually telling you that they're going to track you with a big blue accept button and no real choice at all."¹⁶³
7. If you are not truly provided the choice to accept or deny consenting to the use your person or information, your right to privacy is violated
 - a. Apple: Users must have the choice to allow or not allow apps to track them
8. Because my right to privacy begins with my right to control myself, by "accepting" an agreement to use a third-party app I am not tactically consent, or relinquishing, my right to privacy
 - a. Apple: Applications must put their tracking measures in plain language so that users can understand and consent to being tracked or opt out.

While Apple may not lay out my *privacy-as-property* model in their keynote presentations or policy agreements, my conception of the right to privacy provides the

¹⁶³ "Apple's Craig Federighi Explains iOS 14.5's Privacy Features | WSJ," Wall Street Journal, YouTube, 8:05, April 26, 2021, <https://youtu.be/G05nEgsXgoI>

fundamental reasoning for Apple's privacy changes. Even the late Steve Jobs's view on privacy can be justified by *privacy-as-property*:

"Privacy means people know what they're signing up for, in plain English and repeatedly. That's what it means. I'm an optimist. I believe people are smart and some people want to share more data than other people do. Ask them. Ask them every time. Make them tell you to stop asking them if they get tired of your asking them. Let them know precisely what you're going to do with their data."¹⁶⁴

Choice is undoubtedly essential. Individuals will choose to whether or not to agree to data aggregation as they see fit; however, they must have that choice. So, this privacy feature by Apple is the necessary step forward in the area of privacy. They express that the reasoning for this is that "it's the right thing to give users a choice; regardless of if it's a selling point for phones."¹⁶⁵ It is the right thing to do and it is also a selling point.

More importantly at this current moment Apple is a pioneer among Big Tech. They are putting privacy first and requiring further transparency by third parties. Not all companies are happy. Facebook for one has taken dismay at this new update as their profit-maximizing algorithms abundantly use data tracking to boost advertising profits. Nonetheless, whether corporations willingly welcome this change, whether Apple is now doing what's right, the real truth is that these corporations will have no choice but to emphasize privacy in the coming decade. In the end, the law will eventually correspond to my articulation of *privacy-as-property*. This codification in the law, the true simplicity of understanding the innate right one has to control oneself, will threaten current business practices. In the meantime, the surge in popularity

¹⁶⁴ "D8: Steve Jobs Onstage: Full-length Video," Wall Street Journal, 95:53, June 7, 2010, <https://www.wsj.com/video/d8-steve-jobs-onstage-full-length-video/70F7CC1D-FFBF-4BE0-BFF1-08C300E31E11.html>

¹⁶⁵ "Apple's Craig Federighi Explains iOS 14.5's Privacy Features"

of apps like Signal are bound to absorb some of the market share from big tech if they do not start accentuating privacy.

Ultimately, this advancement in technology companies focus on the right to privacy does not yet follow secure *privacy-as-property*. The reason why the Apple selection appears as “Ask App Not to Track” is because “there are other techniques that developers over time have developed, like fingerprinting, there’s a bit of a cat and mouse game around other ways that an app might scheme to create a tracking identifier, and it’s a policy issue for us to say you must not do that. And so, we can’t ensure at the system level, that they’re not tracking, but we can do so at the policy level.”¹⁶⁶ Therefore third-party apps still have ways to track you, even if you “Ask App Not to Track.” Nonetheless, for all the reasons detailed through this paper, this advancement is an important step forward. Assuredly *privacy-as-property* will prevail, whether or not that specific language is used in future laws.

¹⁶⁶ Apple’s Craig Federighi Explains iOS 14.5’s Privacy Features”

Chapter 13: Conclusion

In 1999, Scott McNealy declared that we “have zero privacy anyway. Get over it.”¹⁶⁷ In 2010 Mark Zuckerberg said that “the age of privacy is over.”¹⁶⁸ In 2014 Thomas Friedman wrote that “privacy is over.”¹⁶⁹ However, they are all wrong, as privacy is very much alive in our society. The issue is that we have simply been looking at privacy through the wrong lenses. For decades we have closely followed the Warren and Brandeis theory of considering privacy as “the right to be left alone.” Scholars have developed this former conception and determined that privacy is synonymous with secrecy; if I am to be left alone, I can live my life free from intrusion. It is not that these conceptions of privacy are completely wrong, but they do become easily antiquated with constant advancements in technology.

Instead, my conception of privacy, a new fundamental approach is timeless. The right to privacy is embedded in a property right to control oneself. Because of this intrinsic right, your property right over yourself extends to your external property, in addition to your cloud data. You must consent to giving away or allowing someone to see your data. In order to consent you must truly have the option, the choice between opting in or out, to the use of data aggregation, artificial intelligence, and data tracking by companies. With this conception of privacy and the innate right to control oneself, when you currently agree to use a third-party, you do not tacitly consent to forego your right to privacy.

¹⁶⁷ Polly Sprenger, “Sun on Privacy: ‘Get Over It’,” *Wired*, January 26, 1999, PM), www.wired.com/1999/01/sun-on-privacy-get-over-it/.

¹⁶⁸ Marshall Kirkpatrick, “Facebook’s Zuckerberg Says the Age of Privacy Is Over,” *Readwrite*, January 9, 2010, https://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov/.

¹⁶⁹ Thomas Friedman, “Four Words Going Bye-Bye,” *New York Times*, May 21, 2014, <https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html>.

This conception of privacy can span generations and will still remain fundamental sound with further advancements in technology. It is my belief that this conception of privacy will be articulated in the law within the next decade. I may be wrong, but it was my desire to prove that this fundamental approach to privacy undoubtedly explains Supreme Court Cases, changes in legislation, and the reasoning for changing business practices.

Technology will unquestionably continue to advance. It will get smarter, faster, and more powerful. It will also pose greater challenges to our right to privacy. Whilst this conception of privacy will remain sound, how can opt-in features be applicable if walking down the street means a facial-recognition technology is providing me with a social credit score.¹⁷⁰ If license plate trackers triangulate my daily travel habits across the city.¹⁷¹ Data sharing in many regards is both beneficial and detrimental to society. It may be the way in which we achieve level five autonomous driving, but it may also be used against individuals to discriminate.

Ultimately, with a fundamental right to privacy articulated throughout the law and changing business practices, institutions spanning from government to for-profits will have to uphold the right to privacy. This change is being accomplished through a combination of market pressure, voluntary restraint, and the looming increase in legislative protections of privacy.

However, this right to privacy doesn't just provide the reasoning for a necessity in altering business practices or legislative change. *Privacy-as-property* can also provide the reasoning for the moral right to privacy when telling secrets to friends and family or even explain the conception of the attorney-client privilege.

¹⁷⁰ Charlie Campbell, "How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens," *Forbes*, <https://time.com/collection/davos-2019/5502592/china-social-credit-score/>.

¹⁷¹ Farivar, *Habeas Data: Privacy vs The Rise of Surveillance Tech*.

So, if my conception does become codified in the law what happens in ten years? If everyone has the option to “opt-in” or “opt-out,” will they choose to opt out, opt in, or will there be a combination of the two? I don’t have the answer to that question, but what is important is that users will have the choice. There will - hopefully - be no forced consent. No large blue box that reads accept while the only other option is to close the website.

However, let's consider a scenario where all users choose to opt-in. In the established conception of privacy, this would mean that they are now freely choosing to have their data tracked and aggregated. This information, which provides insight into our daily life, will still remain its extremely valuable and intimate. Nonetheless, if we made this choice freely, we have now conceded our right to privacy. What protection will our data have then? Would it then be necessary to establish these corporations as information fiduciaries?¹⁷²

Fiduciary law governs patient-doctor relationships, attorney-client privilege, investment advisers, and estate managers.¹⁷³ These laws, a common law creation, ensure that individuals act in the best interest of their patients or clients. They are prescribed with specific duties - fiduciary duties - in respect to their clients’ data, money, and information. In these fiduciary examples the information shared, which can be very personal and intimate, is still considered private. Can we then expect the same out of technology companies? Can we require them to be fiduciaries of our very intimate, and personal data? This would mean that corporations must treat and use our data in our best interests, rather than for their pure monetary gain.¹⁷⁴ Would it then be necessary to hold these large corporations, who make money on scraping user data, even when users opt-in, to the legal standard of a trust fiduciary? I do not have the answer to this question as of yet.

¹⁷² Jack M Balkin, “Information Fiduciaries and the First Amendment,” UC Davis Law Review, Vol. 49, No. 4, (2016): 1183-1234, https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf

¹⁷³ Waldman, *Privacy as Trust*, 85

¹⁷⁴ *Ibid.* 88

Nevertheless, this scenario cannot be possible without the understanding that many current policies do not allow for voluntary consent. Disclosing information to corporations, for the most part, is necessary.

Yet, this will change, *privacy-as-property* will prevail, and we may then be able to consider whether to make tech companies information fiduciaries when users choose to share their data. In the meantime, we must start thinking of *privacy-as-property* and the impact this fundamental approach will have on law and corporations.

Bibliography

Alderman, Ellen and Caroline Kennedy. *The Right to Privacy*. New York: Vintage Books, 1997.

Apple Developer, “App Tracking Transparency,” Apple 2021, <https://developer.apple.com/documentation/aptrackingtransparency>

Apple. “Control personalized ads on the App Store, Apple News, and Stocks.” Published Date: January 7, 2021. <https://support.apple.com/en-us/HT202074>.

Apple. “Data Privacy Day at Apple: Improving transparency and empowering users.” January, 27, 2021, <https://nr.apple.com/dE5w5d0n8O>

Apple. “WWDC 2020 Special Event Keynote — Apple.” YouTube, 1:48:51, June 22, 2020, <https://youtu.be/GEZhD3J89ZE>

Balkin, Jack M. “Information Fiduciaries and the First Amendment.” UC Davis Law Review, Vol. 49, No. 4, (2016): 1183-1234, https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf

Beales, Howard. “The Value of Behavioral Targeting.” *Networking Advertising Initiative*, (2010): 1-24, www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

Calo, M Ryan, “Against Notice Skepticism in Privacy (and Elsewhere),” *NOTRE DAME L. REV.* 87, No.3. (2012): 1027-1072, <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/>

Campbell, Charlie. “How China Is Using “Social Credit Scores” to Reward and Punish Its Citizens.” *Forbes*, <https://time.com/collection/davos-2019/5502592/china-social-credit-score/>.

Carpenter v. United States, 585 U.S. ____ (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Chen, Brian X. “Are Targeted Ads Stalking You? Here’s How to Make Them Stop.” *New York Times*, August 15, 2018, <https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html>.

Chimel v. California, 395 U.S. 752 (1969), <https://supreme.justia.com/cases/federal/us/395/752/>,

Citizens United v. Federal Election Commission, 558 U.S. 310 (2010), <https://www.supremecourt.gov/opinions/09pdf/08-205.pdf>

U.S Department of Health, Education. & Welfare, “Records, Computers, and the Rights of Citizens.” (1973): i-346, Library Department of Justice, www.justice.gov/opcl/docs/rec-com-rights.pdf.

Confessore, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” *New York Times*, April 4, 2018. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

Cranor, Lorrie Faith. “Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice,” *Journal on Telecommunication and High Technology Law* 10, (2012): 273-308. http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Cranor.PDF

Curry, David. “Signal Revenue and Usage Statistics (2020).” *Business of Apps*, March 10, 2021, <https://www.businessofapps.com/data/signal-statistics/>.

Declaration of Independence, July 4, 1776, National Archives, <https://www.archives.gov/founding-docs/declaration-transcript>

Dörr, Dieter and Russell L. Weaver. *The Right to Privacy in the Light of Media Convergence – : Perspectives From Three Continents. Media Convergence / Medienkonvergenz*. Berlin: De Gruyter, 2012.
<http://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=nlebk&AN=471029&site=ehost-live&scope=site>.

Duffy, Clare. “Why messaging app Signal is surging in popularity right now.” *CNN Business*, January 13, 2021, <https://edition.cnn.com/2021/01/12/tech/signal-growth-whatsapp-confusion/index.html>.

Duhigg, Charles. “How Companies Learn Your Secrets.” *New York Times*, February 16, 2012. www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

European Commission. “Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).” Last update April 26, 2021, <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence>

Facebook. “Control the Ads You See.” (2021)
https://www.facebook.com/help/1075880512458213/?helpref=hc_fnav ;

Farivar, Cyrus, *Habeas Data: Privacy vs The Rise of Surveillance Tech*. Brooklyn: Melville House, 2018.

Federal Communications Commission v. AT&T Inc., 562 U.S. 397 (2011)

Federal Trade Commission. “FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.” July 24, 2019, <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>

Friedman, Thomas. “Four Words Going Bye-Bye.” *New York Times*, May 21, 2014, <https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html>.

Goel, Vindu. "Flipping the Switches on Facebook's Privacy Controls." *New York Times*, January 29, 2014, <https://www.nytimes.com/2014/01/30/technology/personaltech/on-facebook-deciding-who-knows-youre-a-dog.html>.

Google. "Block certain ads." <https://support.google.com/ads/answer/2662922?hl=en>

Graham, Megan. "Google says it won't use new ways of tracking you as it phases out browser cookies for ads," March 3, 2021, *CNBC*, <https://www.cnbc.com/2021/03/03/google-says-it-wont-track-you-directly-in-the-future-as-it-phases-out-cookies.html>.

Griswold v. Connecticut, 381 U.S. 479 (1965), <https://supreme.justia.com/cases/federal/us/381/479/#tab-opinion-1945663>

Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (N.H. 1964)

Hirshleifer, Jack. "Privacy: Its Origin, Function, and Future." *The Journal of Legal Studies* 9, no. 4 (1980): 649-64. <http://www.jstor.org/stable/724176>.

In re Snapchat, Inc., FTC File No. 132 3078, No. C- 4501 (F.T.C. May 8, 2014), www.ftc.gov/system/files/documents/cases/14_0508snapchatcmpt.pdf

Intersoft Consulting, "General Data Protection Regulation, Regulation (EU) 2016/679, OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018." <https://gdpr-info.eu/>.

James Madison, *Property* (1792), (rp: The Founders' Constitution, Philip B. Kurland & Ralph Lerner eds.) The University of Chicago Press (1977), <http://press-pubs.uchicago.edu/founders/documents/v1ch16s23.html>.

Kirkpatrick, Marshall. "Facebook's Zuckerberg Says the Age of Privacy Is Over," *Readwrite*, January 9, 2010, https://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov/.

Lee Raine and Maeve Duggan, "Privacy and Information Sharing," *Pew Research Center* (2016): 1-46, www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

Locke, John. *Second Treatise of Government*. (1980) Edited by C. B. Macpherson. Cambridge, MA: Hackett Publishing

M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Available at: <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3>

McDonald, Aleecia M. and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies, *A Journal of Law and Policy for the Information Society*," vol. 4, no. 3 (2008): 543-568. <http://hdl.handle.net/1811/72839>

Mozur, Paul, Kang, Cecilia, Satariano, Adam and David McCabe. “A Global Tipping Point for Reining In Tech Has Arrived.” *New York Times*, April 20, 2021, <https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html>.

Office of the Privacy Commissioner of Canada, “PIPEDA in brief.” Revised May 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Office of the Privacy Commissioner of Canada. “The Privacy Act in brief.” August 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

Oxford English Dictionary Online (OED Online), 2021 Oxford University Press, <https://www.oed-com.ccl.idm.oclc.org/>

Page, Carly. “WhatsApp Delays Privacy Changes Amid ‘Confusion’ About Facebook Data-Sharing.” *Forbes*, January 15, 2021, <https://www.forbes.com/sites/carlypage/2021/01/15/whatsapp-delays-privacy-changes-amid-confusion-about-facebook-data-sharing/?sh=16a114674dbc> (PM), www.wired.com/1999/01/sun-on-privacy-get-over-it/.

Riley v. California, 573 U.S. 373 (2014), https://www.supremecourt.gov/opinions/13pdf/13-132_819c.pdf

Roose, Kevin. “A Machine May Not Take your Job, but one could become your boss.” *New York Times*, June 23, 2019, <https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html>.

Satariano, Adam. “Europe Proposes Strict Rules for Artificial Intelligence.” *New York Times*, April 21, 2021, <https://www.nytimes.com/2021/04/16/business/artificial-intelligence-regulation.html>.

Signal (App). <https://www.signal.org/>.

Signal Foundation. <https://signalfoundation.org/>.

Smith v. Maryland, 442 U.S. 735 (1979), <https://supreme.justia.com/cases/federal/us/442/735/>

Smith, Adam, *Lectures on Jurisprudence* (1763), (ed by. R. L. Meek, D. D. Raphael, and Peter Stein) Oxford University Press: The Glasgow Edition of the Works and Correspondence of Adam Smith, Vol. 5: Lectures on Jurisprudence (1978)

Sprenger, Polly. “Sun on Privacy: ‘Get Over It’.” *Wired*, January 26, 1999,

Steiner, Peter “Cartoon: On the Internet, Nobody Knows You’re a Dog,” *New Yorker*, July 5, 1993.

Stone, Zara. “Daughter Of Fired iPhone X Apple Engineer Is Really, Really Sorry.” *Forbes*, October, 31, 2017, <https://www.forbes.com/sites/zarastone/2017/10/31/daughter-of-fired-iphone-x-apple-engineer-is-really-really-sorry/?sh=446cf169ad76>.

Su, Jeb. “Confirmed: Apple Caught In Siri Privacy Scandal, Let Contractors Listen To Private Voice Recordings.” *Forbes* July, 30, 2019, <https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/?sh=48f894077314>

Su, Jeb. Why Amazon Alexa Is Always Listening To Your Conversations: Analysis.” *Forbes*, May 16, 2019, <https://www.forbes.com/sites/jeanbaptiste/2019/05/16/why-amazon-alexa-is-always-listening-to-your-conversations-analysis/?sh=6e1abe7e2378>

Twitter. “Your privacy controls for personalized ads.” <https://help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads>

United States v. Jones, 565 U.S. 400 (2012), <https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>

Upper Canada College. “Edward Snowden Speaks to World Affairs Conference 2015,” YouTube video, 1:33:32, YouTube, 3 Feb. 2015, www.youtube.com/watch?v=JXplakuhjL8.

Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age*, Cambridge: Cambridge University Press, 2018.

Wall Street Journal “D8: Steve Jobs Onstage: Full-length Video.” WSJ Video, 95:53, June 7, 2010, <https://www.wsj.com/video/d8-steve-jobs-onstage-full-length-video/70F7CC1D-FFBF-4BE0-BFF1-08C300E31E11.html>

Wall Street Journal, “Apple’s Craig Federighi Explains iOS 14.5’s Privacy Features | WSJ,” Wall Street Journal, YouTube, 8:05, April 26, 2021, <https://youtu.be/G05nEgsXgoI>

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review*, vol. 4, no. 5, (1890): 193–220, www.jstor.org/stable/1321160

Weeks v. United States United States, 232 U.S. 383 (1914), <https://supreme.justia.com/cases/federal/us/232/383/>

Wyoming v. Houghton, 526 U.S. 295 (1999), <https://supreme.justia.com/cases/federal/us/526/295/>

Yarrow, Jay. “What It’s Like on Day One as an Apple Employee.” *Business Insider*, January 26, 2012, www.businessinsider.com/what-its-like-on-day-one-as-an-apple-employee-2012-1.