1

Introduction

There is a myth – perhaps you saw a version of it in the movie *Braveheart* – told about the abuses of feudal lords, about the *droit du seigneur* or *ius primae noctis*: the "right of the lord" or the "right of the first night." A feudal lord supposedly had the right to sexual relations with the bride of a newly married peasant couple. The lord's power over the land on which his tenants lived and worked extended, in this story, to the power to interfere in even the most intimate and personal moments of a couple's lives. The story is just a myth – there is no record of the *ius primae noctis* being exercised in medieval times. It seems to have developed later as a popular and salacious description of the boundless arrogance and power of feudal lords over every detail of the lives of those who lived on their land.

But *this* is no myth: on September 13, 2016, as I was finishing this book, the *Chicago Tribune* reported that a class action lawsuit had been filed on behalf of tens of thousands of people against the makers of WeVibe, a popular couples' erotic massage device.[1] WeVibe was discovered to have been extracting the most intimate data possible from the device: date and time of each use, level of vibration intensity, vibration mode or pattern selection, even the temperature of the device and the email address of the user. The data were apparently collected for purposes of market research. The manufacturer of WeVibe – a company called Standard Innovation – was able to do this as a technical matter because the device was web-enabled, controlled wirelessly by a smartphone application, called We-Connect. Standard Innovation buried software in the device that communicated the intimate details to We-Connect, and We-Connect then secretly forwarded the details to SI's own servers. SI claimed the

[1] *See* Robert Channick, *Lawsuit Claims Smartphone-Enabled Massage Device Violated Privacy*, Chi. Trib. (Sept. 13, 2016, 1:41 PM), http://www.chicagotribune.com/business/ct-vibrator-app-lawsuit-0914-biz-20160913-story.html.

legal right to do this because of terms hidden deep within the app's software license. Never mind that no one reads such terms, or that no one could understand them even if they did. Standard Innovation believed that merely by installing and using its app, users agreed to permit the company to intrude and spy on communications between themselves and their lovers.

This is digital *ius primae noctis*. With all of the brazen arrogance of a digital feudal lord toward his peasantry, SI felt justified in conducting the most gross invasions of privacy and property, in surveilling the most intimate moments between its customers, merely because of the power it holds as the owner of the intellectual property embedded in the device, and as the drafter of clauses buried deep within its license agreement.

Despite the surface flash of a life enhanced by new technologies, the laws and logic that undergird it are made of old and problematic material drawn from a time when many owned little and a few controlled much. The digital and smart devices that surround us are legion, but we do not truly own or control them; the companies that wrote the software inside do.[2] Intellectual property and contract law have crowded out everyday property ownership.

As I describe in this book, with every new push of software into everyday life, the owners of intellectual property assert more control over the daily lives of people who use their products.[3] Smart televisions report on the conversations of people who are merely standing within earshot.[4] Smartphones report the real-world location of users to manufacturers, operating system designers, and app providers.[5] The supposed owner often has less say in what a device or product is doing than does its manufacturer. The "owner" is a source of data to be harvested. As one commentator put it, many social networks and

[2] *See, e.g.*, *PLAYSTATION®4 SYSTEM SOFTWARE LICENSE AGREEMENT (Version 1.1)*, Sony Comput. Ent. Inc. (2015), http://www.scei.co.jp/ps4-eula/ps4_eula_en.html ("All rights to use [the PS4] System Software are granted by license only, and you are not granted any ownership rights or interests in System Software."). The PS4 agreement further provides: "If SCE determines that you have violated this Agreement's terms, SCE may itself or may procure the taking of any action to protect its interests such as disabling access to or use of some or all System Software . . . or reliance on any other remedial efforts as reasonably necessary to prevent the use of modified or unpermitted use of System Software." *Id*.

[3] *See generally* Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 Berkeley Tech. L.J. 55 (2012).

[4] *See* Dave Lewis, *Is Your TV Spying on You?*, Forbes (Feb. 10, 2015), http://www.forbes.com/sites/davelewis/2015/02/10/is-your-tv-spying-on-you (noting that Samsung's privacy policy provides that "when you watch a video or access applications or content provided by a third-party, that provider may collect or receive information about your SmartTV . . . and your use of the application or service," and that "Samsung is not responsible").

[5] *See* J.D. Harrison, *Companies Know Where You Went Online. Now, They Can Follow You Around in Real Life*, Wash. Post (Apr. 10, 2015), https://www.washingtonpost.com/news/on-small-business/wp/2015/04/10/companies-know-where-you-went-online-now-they-can-follow-you-around-in-real-life-too (discussing businesses' use of location-based data analytics).

search engines "have turned into nothing more than the 21st century's mining companies, constantly mining for the next nugget of gold."[6]

We own and control fewer and fewer of the products that we must use to function in modern society. Many computing devices (iPads, for instance) run only those programs approved by the device seller. We cannot even tell our devices not to reveal our personal data.[7] The only guaranteed way to stop a smartphone from reporting on our web searches, web traffic, real-world location, texts, and surrounding ambient sounds and sights is to pull out its battery or not to carry one. This is an untenable position in an information-age society. In the United States alone, two-thirds of Americans own a smartphone and use it as "a key entry point to the online world."[8]

To be clear, I am no Luddite. Technology itself is not the problem. The problem is when our devices serve the companies who made them rather than the people who purchased them. And as our bridges and our bodies, our school buses and our supermarkets, our keychains and our grills become colonized with digital connections and capabilities – an infrastructure of networked sensors, software, electronics, and apps otherwise known as the Internet of Things – the question of control becomes only more significant.

To fix this, we must re-establish control of our digital and smart property at the most basic level. We must restore everyday property ownership. If we do not take back our ownership rights from software companies and overreaching governments, we will become digital peasants, only able to use our smart devices, our homes, our cars, and even our own software-enabled medical implants purely at the whim of others. Like the serfs of feudal Europe who lacked rights in the land they worked, without digital property rights, we aren't owners – we're owned.

The act of owning works considerable social magic. Private property performs an important role in balancing the parts that citizen, corporation, and state play in relation to one another in modern society.[9] Well-defined property rights spur investment. By controlling resources, owners may control their

[6] Henk Campher, *Data Mining: The Consumer Becoming the Consumed*, Huffington Post (Oct. 8, 2014), http://www.huffingtonpost.com/henk-campher/data-mining-the-consumer-_b_5949580.html.

[7] *See* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, Wall Street J. (Dec. 17, 2010), http://www.wsj.com/articles/SB10001424052748704694004576020083703574602 (noting that an investigation "showed that 56 [apps] transmitted the phone's unique device ID to other companies without users' awareness or consent").

[8] *See* Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Res. Ctr. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015.

[9] *See, e.g.*, Benjamin Powell, Private Property Rights, Economic Freedom, and Well Being 1 (Mercatus Ctr. at George Mason Univ., Working Paper No. 19, 2003), http://mercatus.org/sites/default/files/Private-Property-Rights-Economic-Freedom-and-Well-Being.pdf ("Observation of the countries around the world also indicates that those countries with an institutional

own destinies (or at least attempt to do so). Furthermore, owners can order their surroundings to their liking by modifying their property. An owner might repaint the walls of her room bright neon green. She might soup up the engine of her truck to make it less fuel-efficient but more powerful. She might plant a vegetable garden on her land, if she desires carrots, or plant flowers, if she decides otherwise. In other words, the control over surroundings that basic ownership supplies is linked to the democratic value of self-determination. There are other ways to provide this self-determination and control, to be sure – for example, with a focus on human rights.[10] But those systems cannot entirely replace simple, robust, old-fashioned ownership.

Property also works economic magic. Purchasing property is in many cases like taking money out of one's left pocket only to have it reappear in the right. Consider the act of buying and owning a house: the purchaser pays a monthly mortgage payment but, ideally, also builds equity in the house, which can be drawn upon in time of need. Yet new forms of property, such as Kindle e-books, come in forms that do not build or retain wealth; they cannot be resold.[11] Worse still, once consumers have built up libraries of Kindle e-books, they are subject to lock-in effects: if consumers shift to another device or service, they cannot take their library with them.[12]

These may seem like trivial things – who really counts the value of her book collection in her overall wealth anyway? – but software governance and the intellectual property rules that accompany them are infiltrating more economically important purchases, like houses, cars, and industrial equipment.[13] If those assets cannot be owned, the primary forms of wealth held by a large

environment of secure property rights and high degrees of economic freedom have achieved higher levels of the various measures of human well being.").

[10] *See* G.A. Res. 1514 (XV) (Dec. 14, 1960) ("All peoples have the right to self-determination; by virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.").

[11] *See, e.g.*, *Kindle Store Terms of Use*, Amazon (last updated Mar. 15, 2016), http://www.amazon.com/gp/help/customer/display.html?nodeId=201014950 ("Unless specifically indicated otherwise, you may not sell, rent, lease, distribute, broadcast, sublicense, or otherwise assign any rights to the Kindle Content or any portion of it to any third party, and you may not remove or modify any proprietary notices or labels on the Kindle Content.").

[12] In other words, those who invest in their Kindle e-book library are stuck using Kindle, even if at some later date they would prefer to use another e-book management system. *See* Dan Costa, *Nook, Kindle and the Perils of Lock-in*, PC Mag. (June 1, 2011), http://www.pcmag.com/article2/0,2817,2386266,00.asp (noting that lock-in "makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs.").

[13] One notable example, explored further in later chapters, is tractors, which "are increasingly run by computer software." Laura Sydell, *DIY Tractor Repair Runs Afoul of Copyright Law*, NPR (Aug. 17, 2015), http://www.npr.org/sections/alltechconsidered/2015/08/17/432601480/diy-tractor-repair-runs-afoul-of-copyright-law.

section of the population will simply vanish. What would happen if the rules that govern a smartphone (for example, you cannot modify the phone's software without hacking it; cannot effectively block surveillance; and must submit to having your information given to hundreds of advertisers) become the rules that govern your software-enhanced self-driving car or smart house?

The future of basic ownership rights in digital and smart property is uncertain and precarious because of two historical developments. First, internet technologies created an unprecedented ability to copy intellectual property – file sharing services spread pirated music like wildfire and fueled the music industry's fears for its own future[14] – before they created the ability to track and verify individual copies of electronic information.[15] In the absence of a company's ability to ascertain that Book A is actually John's book, and not merely a book that John has instantly and cheaply copied from Mary, intellectual property owners instituted a range of command-and-control powers in their software. Thanks to subsequent federal legislation, those controls came to be backed by a host of incredibly strong legal powers.[16]

This gave rise to both opportunism and missed opportunities. Companies opportunistically used these powers not just to fight piracy but also to lock owners out of their own property. Meanwhile, courts missed the opportunity to adapt the law of traditional ownership – property law – to new digital assets and smart property. The reasons for this are complex, but one consistent issue is that courts have struggled to define traditional property interests in intangibles – things that you cannot touch, weigh, or feel – while also honoring intellectual property concerns. This left a void in the law, a void filled by overextended intellectual property law, which further strengthened the power of companies to control consumers' property. What is needed – and what I attempt to provide in this book – is not merely an argument for reining in overreaching intellectual property law, but the development of a real alternative: a convincing theory of intangible property that courts can use to support consumers' claims of ownership.

The second development affecting the future of ownership rights was similar but distinct. Initially, consumers were not used to paying for internet-based

[14] *See* Eduardo Porter, *The Perpetual War: Pirates and Creators*, N.Y. Times (Feb. 4, 2012), http://www.nytimes.com/2012/02/05/opinion/sunday/perpetual-war-digital-pirates-and-creators.html.

[15] *See generally* Bill D. Herman, *A Political History of DRM and Related Copyright Debates, 1987–2012*, 14 Yale J. L. & Tech. 162 (2012) (providing a history of DRM and copyright).

[16] *See, e.g.*, *The Pros, Cons, and Future of DRM*, CBC News (Aug. 7, 2009), http://www.cbc.ca/news/technology/the-pros-cons-and-future-of-drm-1.785237 (noting an incident where "Amazon used its DRM technology to remotely delete copies of George Orwell's 1984 and Animal Farm novels from users' Kindle e-book readers without their knowledge or consent").

services.[17] Business models of all kinds had to adapt to find new income streams. Newspapers were forced to rethink their operations and revenue structures because online users were used to getting content for free.[18] Likewise, software providers needed a revenue model that circumvented internet users' refusal to pay for content that they could obtain – usually illegally, but with some degree of safety – for nothing.[19] So software providers monetized information about their consumers by surreptitiously monitoring everything their users typed, clicked, or did, and selling that information to advertisers, who could use it to extract more and often costlier deals from their customers.

Information about consumers became the currency of the internet, and commercial surveillance became its funding model.[20] User information was increasingly gathered by software embedded first in internet websites,[21] and later into the very devices that consumers purchased to access and use internet technologies.[22] That information could then be monetized through targeted behavioral advertising.[23] By watching everything a consumer did, an advertiser could make enough enhanced revenue through targeted sales that it was willing to provide the relevant software (say, the operating system for a mobile smartphone) at a steep discount – or subsidize it for software companies. This is how Facebook monetized its services.[24] By knowing everything about the consumer, companies could charge consumers more if they were likely to pay more (Mac users pay more for hotel rooms booked online[25]), or offer

[17] *See* Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World 50 (W.W. Norton and Company 2015) ("Before 1993, the Internet was entirely noncommercial, and free became the online norm.").

[18] *See* Rachel Smolkin, *Adapt or Die*, Am. Journalism Rev. (June 2006), http://www.ajrarchive.org/Article.asp?id=4111 (discussing the trend of newspapers transforming "from newspaper companies to information companies" in the mid-2000s due to more prevalent internet usage).

[19] *See, e.g.*, Schneier, *supra* note 17, at 48 (noting that even the free game Angry Birds "collected location data").

[20] *See id.* at 49 (describing "[s]urveillance" as "the business model of the Internet").

[21] *See id.* at 48–49 (discussing the history of "third-party cookie[s] . . . tracking web users across many different sites" and noting that, based on 2010 data, even "a seemingly innocuous site like Dictionary.com installed over 200 tracking cookies on your browser when you visited").

[22] *See id.* at 59 (discussing "the rise of user devices that are managed closely by their vendors").

[23] *See id.* at 53–56 (discussing the use of "commercial surveillance data" in targeted advertising).

[24] *See* Geoffrey A. Fowler, *What You Can Do About Facebook Tracking*, Wall Street J. (Aug. 25, 2014), http://www.wsj.com/articles/what-you-can-do-about-facebook-tracking-1407263246 ("[Facebook's] main business is selling marketers access to you, but it does this without telling them who you are.").

[25] *See* Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, Wall Street J. (Aug. 23, 2012), http://www.wsj.com/articles/SB10001424052702304458604577488822667325882 ("Orbitz Worldwide Inc. has found that people who use Apple Inc.'s Mac computers spend as much as 30% more a night on hotels, so the online travel agency is starting to show them different, and sometimes costlier, travel options than Windows visitors see.").

consumers deals that they would be unlikely to resist (comparison shoppers pay more for airfare because their browser histories indicate they are very interested in certain flights[26]). The consumer therefore does not pay directly for use of internet technologies, but pays by being surveilled to such an extent that she may engage in an increased number of costlier deals than would have been the case had she not been subject to surveillance by her own devices.

What began as simple exchange – information for valuable goods and services – has escalated to exploitation. A 2014 Pew survey indicates that 91 percent of respondents felt that they have lost control over what information is gathered, how it is gathered, to whom that information is revealed, how long that information may be used, and how far the information can travel.[27] The combination of loss of control over our devices and exploitation of the data our devices gather about us could yield a grim future, one in which there is no escape from the many devices that each person carries with them, or that other people carry, or that lie in wait wherever we go in an increasingly ubiquitous computing environment.

Escaping a network of integrated things designed from the ground up to leak information about their supposed owners will not be easy. Steering the Internet of Things away from its anticipated near-future as a distributed, mobile, and pervasive surveillance network will take some doing. But, as I argue in this book, escape is possible. Technologists have created tools to help handle the twin problems of piracy and payment that have caused intellectual property owners to assert such control over networked devices.[28] It is now possible to have a reasonable economy not predominantly based on exploitation of consumer information.

There is a narrow temporal window that is rapidly closing. Privacy is a scarce and precious social value. As our personal information becomes increasingly digitized, there is a growing concern not just about who collects our data, but what they collect.[29] We are learning helplessness in the face of rampant spying

[26] *See* Annie Lowrey, *How Online Retailers Stay a Step Ahead of Comparison Shoppers*, Wash. Post (Dec. 11, 2010, 5:32 PM), http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121102435.html (explaining the process behind the "experience of buying a plane ticket through a portal such as Kayak, then seeing the final price jump $10 or $40 at check out").

[27] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Res. Ctr. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions.

[28] Cryptographic ledgers, for example, make it possible to transfer a specific single copy of digital property. This recording system will be further explained in Chapter 7.

[29] *See* Mary Madden & Lee Raine, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance ("90% of adults say that controlling what information

by the devices that surround us. We value privacy highly – in a recent survey, 93 percent of adults said that being in control of who can get information about them is important.[30] But as we realize our efforts to procure privacy are costly and fruitless, we may learn to stop trying.[31] This will cause further erosion – not of our desire for privacy, but of our efforts to obtain it or pay for it. If society truly teaches its citizens that the devices they own will inevitably be controlled not by them, but by corporations and government, then citizens will stop investing in the few technologies, devices, and services that attempt to provide even some small amount of control.

What is needed is an escape mechanism – a way out of the trap of device-based surveillance. This book proposes that such an escape would have four necessary components. They are simple extensions of the property rights that people have traditionally enjoyed over their possessions. First, people have the right to modify their own property.[32] Second, they can sell it to others, free and clear, when they are done with it. Third, they can use it and enjoy it free from the interference of others.[33] Fourth, they can exclude others from using it without their consent.[34] These four basic rights that all of us have over our ordinary property – the right to modify, the right to sell, the right to use, and the right to exclude others – are the foundation of this book's attempt to create a metaphorical escape button for an Internet of Things that overrides personal control and ownership.

In the online and digital landscape – a terrain increasingly synonymous with the "real" one – these traditional rights of ownership translate into the rights to hack, sell, run, and ban. Briefly, people must first be able to control, modify, and reprogram their devices: a "right to hack." People must be legally and technologically enabled to modify, destroy, reprogram, rework, upgrade, and change their devices to fit their own needs. There is growing support for this right: "jailbreaking" your iPhone or rooting your smartphone are necessary and popular actions. In fact, in 2015 the U.S. government granted consumers

is collected about them is important; 65% think it is 'very important,' while only 25% say it is 'somewhat important.'").

30 *See id.* ("93% of adults say that being in control of who can get information about them is important; 74% feel this is 'very important,' while 19% say it is 'somewhat important.'").

31 *See* Schneier, *supra* note 17, at 59–61 (discussing the inability of consumers to resist the privacy-invading rules set by technology vendors).

32 *See* 63C Am. Jur. 2d Prop. § 1 (2008) ("Ownership of property implies the right of possession and control.").

33 *See id.* ("Generally, the common law concept of 'property' refers to the right and interest that a person has in an object, which extends beyond ownership and possession to include the lawful, unrestricted right of use, enjoyment, and disposal of the object.").

34 *See id.* (noting that "the right to exclude persons is a fundamental aspect of private property ownership").

the right to jailbreak their smartphones, despite Apple's disapproval of the practice.[35] Intellectual property interests that obstruct the right to hack must give way. People must be able to modify their devices to stop them from leaking data to every app and service provider, should they wish to do so. Companies' promises about how they use our data are intentionally vague and filled with weasel words. The only way to ensure data security is to block the data flows at our end, on our own devices.

Second, I propose a "right to sell." A primary characteristic of property is that it can be sold to someone else. Copyright holders and digital service providers want to destroy markets for used goods so that they can make more sales. If Apple were to get rid of CDs on eBay, it could sell more music. Amazon does not want you selling your used Audible recordings or e-books when you are done with them: that is a sale it does not get. But secondary markets are good for consumers, and are well-established mechanisms for the turnover of property. We buy used goods on eBay because prices are lower. And, of course, consumers benefit doubly from consumer-to-consumer sales, because one consumer is happy to get rid of her old junk, and another is happy to get a great deal on something that is (to her) new and perhaps unavailable elsewhere.

Letting consumers sell their digital assets also impedes the lock-in effect. If you don't like one service, you should be able to sell your account and go elsewhere, just as if you sold your house in a gated community with an overly intrusive homeowners' association. You do not have to burn down your house to move; even the most meddlesome HOA does not have the capacity to forbid the sale of the property you own under its umbrella. In the same way, you should not have to delete your account, Audible downloads, MP3s, software, or e-books, or consign them to the digital dustbin; you could simply get some of your money back out by selling them to someone else. The right to sell protects consumers from attractive-looking offers that turn out poorly, or lets them free up money from things they no longer need.

Third, we must have the right to use our own property as we see fit, to run whatever code we like: a "right to run." Apple controls which software can run on its devices.[36] Often this protects customers from threats – invasive third

[35] *See* Andrea Peterson, *New iOS Malware Should Make You Think Twice About Jailbreaking Your iPhone*, Wash. Post (Sept. 1, 2015), http://www.washingtonpost.com/news/the-switch/wp/2015/09/01/new-ios-malware-should-make-you-think-twice-about-jailbreaking-your-iphone (noting that "the Librarian of Congress . . . approved an exception to the Digital Millennium Copyright Act, allowing consumers to jailbreak their smartphones," but that "Apple discourages the practice").

[36] *See id.* ("Apple keeps tight control over what apps are allowed on iPhones, running basic security tests before allowing them to be downloaded.").

parties, for example[37] – but just as often it locks the customer into running only programs approved by Apple, created by vendors who give Apple a cut and do not compete with Apple in its core business interests.[38] Citizens must have rights in software-enhanced and digital property that do not vanish at the sole discretion of intellectual property rightsholders.

Fourth and finally, we must be able to exclude intruding data collectors from our property.[39] An endless string of user agreements, intentionally complicated privacy controls, privacy policies that do not protect privacy, and, above all, devices that have been designed to leak information about the user at every level – hardware, firmware, operating system, user interface, and over-the-wire communication – make it infeasible for users to exercise their basic option to exclude. Yet the right to exclude is the most basic property right of all.[40] It is the right to stop other people from using property against the owner's wishes, or in the case of smart property, against the owner herself. I propose a "right to ban," to give full force and effect to users' rights to exclude companies who would subvert users' property to their own purposes. By giving users the legally enforceable right to say no to intrusion, law would effectively give them the right to exclude.

Sir William Blackstone, the giant of the common law, wrote: "There is nothing which so generally strikes the imagination, and engages the affections of mankind, as the right of property; or that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[41] I have always thought the second part of that quote got too much play. Our property is not ours to do with as we absolutely please. I cannot erect a

[37] *See* David Goldman, *Apple Bans Hundreds of iPhone Apps That Secretly Gathered Personal Info*, CNN (Oct. 19, 2015), http://money.cnn.com/2015/10/19/technology/apple-app-store (noting that Apple removed from its app store a number of apps which "gathered information about the people who downloaded the apps, including their email addresses and iPhone serial numbers").

[38] *See* Kushal Dave, *Apple's App Store Review Process Is Hurting Users, but We're Not Allowed to Talk About It*, Bus. Insider (Apr. 12, 2015), http://www.businessinsider.com/apples-app-store-review-process-is-hurting-users-but-were-not-allowed-to-talk-about-it-2015-4 ("Apple prohibits in-app purchases it can't get its 30% cut of, leading to a situation where users cannot buy books in their Kindle app or videos in their YouTube app or comics in their comics app, even though they can on Android. In the early days of the app store, Apple rejected apps just for competing with their own built-in apps.").

[39] *See* Schneier, *supra* note 17, at 59–61 (discussing the difficulty of preventing unwanted data collection).

[40] *See* 63C Am. Jur. 2d Prop. § 1 (2008) ("The right to exclude others, as well as their property, is one of the most essential sticks in the bundle of rights that are commonly characterized as property.").

[41] 2 William Blackstone, Commentaries *2.