EDITORS: Rick Kuhn, US National Institute of Standards and Technology, kuhn@nist.gov
Tim Weil, US Department of Interior, trweil@ieee.org

Protecting Digital Assets

Legal Protections ≠ Practical Security

Joseph Webster, Max Romanik, and Christopher Webster, *ShieldMyfiles*

The Internet is a lawless place. Before the digital era, items such as books, photographs, and mail were all owned in the physical world. Physical ownership comes with legal protections against theft, misappropriation, and seizure. As books become e-books, cameras become just another connected Web application, and communications become entirely digital, the law struggles to apply traditional legal concepts of privacy and property ownership to digitization. Here, we examine the ways in which traditional legal protections fail to meet the needs of digital property owners, looking first at two legal concepts relevant to protecting digital assets. We then examine how these laws apply—or don't—to data in the digital world.

Ownership

Legal ownership of property can be best described as a bundle of exclusive rights, including possession, use, and disposition.[1] Strong property rights exist when a single person or entity can substantiate that he or she has actual and exclusive possession of, is in use of, and is free to dispose of a given piece of property. The old adage "possession is nine-tenths of the law" does not mean that use and disposition are worth only one-tenth of a legal property claim. Rather, possession presents a rebuttable presumption that the possessor is indeed the lawful owner.[2] Take, for example, a Ferrari—the driver in possession is presumed to be the lawful owner.

The full bundle of rights is difficult to effectuate in our modern digital world. For example, in the case of the digital file "example.txt," the file's original creator is in exclusive possession, can use the file in any way he or she wishes, and is free to dispose of the file by sale, deletion, copying, sharing, and so on. This seems like a clear-cut example of property rights in practice. Digital assets, however, have certain characteristics that physical or analog property do not. File duplication is one characteristic that makes enforcement of classic property rights less certain. Duplication defeats exclusivity of possession because a copied file can be held by multiple users who can use or dispose of it in any way they wish. Contrast this digital reality with the physical realities of any piece of tangible property, like our Ferrari. The Ferrari cannot be copied for personal gain, stored all over the world, and seamlessly replaced when lost.

The Fourth Amendment

In addition to property law, digital assets can fall under the protections of the Fourth Amendment to the US Constitution, which provides protections from the US government. To fall under this protection, digital assets must be entitled to a "reasonable expectation of privacy."[3] More specifically, an owner must exhibit "an actual expectation" of privacy, and that expectation must be one "that society is prepared to accept."[4] Simply put, to have an expectation of privacy owners must take some steps to protect their property, and those steps must be ones that are recognized by society as valid means of protecting the privacy of that property (for example, storing documents in a locked safe).

 Published by the IEEE Computer Society

Data at Rest

It is difficult to apply the laws of property ownership and Fourth Amendment privacy protections to the digital world. The relationship between users and cloud services aptly illustrates these difficulties. This relationship is defined by the contract for services that is accepted when the user establishes an account. The service is a third party to whom users are voluntarily giving stewardship of some of their digital property. Contained in a typical set of terms are a number of provisions that are inconsistent with full property ownership. Google's terms of service state, "you retain ownership of any intellectual property rights that you hold in [your] content. In short, what belongs to you stays yours." But these terms also grant to Google a "worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publicly perform, publicly display, and distribute such content" (see www.google.com/intl/en/policies/terms/). The first clause creates and maintains the user's property rights, but the second is inconsistent with notions of sole ownership. While cloud providers such as Google would not be able to provide their products and services without this broad license, the result is that exclusive ownership is not held by the user. Rather, this is shared ownership in which users give up some portion of their rights. Additionally, cloud providers are not governmental entities. Thus, Fourth Amendment protections are not available to users, who have already consented to cloud providers viewing, using, hosting, storing, and modifying their files.

Worse yet, if the government wants to seize a user's files from a cloud provider, it can compel the provider to turn over files—in some cases without a warrant! The Stored Communications Act[5] presents two methods for the government to seize and search stored electronic records. If the records have been stored for less than 180 days, a warrant is required in all circumstances. If the records have been stored for 180 or more days, the government has three options: seize with a warrant, and demand that the user not be notified of the seizure indefinitely; seize with an administrative subpoena, and demand that the user not be notified of the seizure for 90 days; or seize with a subpoena, and within 90 days, file a warrant for the same records, providing the ability to extend the 90-day notice delay indefinitely.[5]

Contrast cloud data with property that is locked in a filing cabinet: the contents of the cabinet are free from prying eyes; the cabinet maker does not search the contents in return for providing the key; and if the government wishes to gain access to the cabinet, it must obtain a warrant based on probable cause. Another, more analogous example is a safety deposit box—the critical similarity being the hiring of a third party to act as a steward. Here, terms of service do not grant the bank license to use the contents of the box. Banks do not view, scan, copy, share, or transport any of the items in the box; the bank cannot inform on you about the contents of the box to intellectual property rights holders.

Data in Motion

The development of modern legal doctrine around the privacy of property in transit began with the US Postal Service (USPS). Since the nineteenth century, the US Supreme Court has accepted that envelopes and other packaging, which shield a parcel's contents from plain sight, create a reasonable expectation of privacy.[6] The only features of these forms of communication that are subject to inspection are the "outward form and weight."[6] In *Ex Parte Jackson*, the Court specifically pointed out that a distinction must be made between mail that is intentionally shielded from inspection, such as letters and sealed packages, and mail that is open to inspection, like magazines or post cards. The constitutional guaranty of privacy attaches to a person's property "where ever [it] may be," including while in transit with the USPS.[6] Mail in transit may only be opened and examined under a warrant "particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."[6] This law is not antiquated; rather, it forms the bedrock on which more modern recitations of the rule are built.[7]

Digital communications (that is, data moving over any common networking protocol) do not cleanly fit this constitutional standard because the Internet was built to be public by design. The USPS was designed to protect the privacy of sealed packages with locked mailboxes, secure sorting facilities, and its own police force. The Internet is replacing secure networks such as the USPS, even though many of the privacy and security mechanisms haven't been addressed. The incongruity between the public design of the Internet and the now private desires of its users creates a legal and regulatory gulf.

Communications routing information does not experience a reasonable expectation of privacy[8]; as such, physical addresses or dialed phone numbers are not private. Accordingly, many courts cast packet metadata in the same light. After all, how could information freely shared with the network and its participants enjoy any

expectation of privacy? Theoretically, this seems like a reasonable extension of the rule; however, it incorrectly analogizes packet metadata with phone numbers or address information. Packet metadata conveys more information than the simple "to" and "from" data that is found in addressing information. In aggregate, it can paint complex maps of interconnection and association that can intrusively reveal far more than simple addressing information about the parties involved. Furthermore, unlike mail sent through USPS, Internet traffic is not carried by delivery agents; it is designed to route packets publically through a flexible patchwork of nodes. Thus, the routing that makes the Internet possible comes at a privacy cost—it reveals packet data to every Internet routing participant.

The revelations by Edward Snowden regarding practices at the US National Security Agency (NSA) demonstrate how widespread bulk metadata collection programs have become. As authorization for the bulk collection of packet metadata, the NSA used the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (or "Patriot Act").[9] It is now expired, but was updated as the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (or "USA FREEDOM Act").[10] With its expiration, the challenges regarding the constitutionality of the Patriot Act are settled (likely candidates include *ACLU v. Clapper*, no. 13-3994, 2013; *Klayman v. Obama*, no. 13-0881, 2013; and *Smith v. Obama*, no. 14-35555, 2014). However, the legal precedent equating metadata with dialed phone numbers[8] remains unchallenged because the data is publicly known and required to route transmissions (follow the appeals of *ACLU v. Clapper*).

Additionally concerning is the fact that more than just packet metadata gets trapped, copied, and read by third parties. In fact, deep-packet inspection is an increasingly important network administration tool, used commonly in firewalls and data-loss-prevention systems. While packet capture might not be the product of malfeasance, it is inconsistent with the basic principles of property ownership and constitutional notions of privacy. Returning to the mailed letter analogy, there is an expectation, both practically and at law, that a mail carrier will not open a sealed envelope, make copies of the contents to read and store, and then reseal the envelope before delivery. In fact, such mail tampering would be a federal crime. Here again, we see the conflict between classical property rights and their application to the digital world.

Legal Protection ≠ Practical Protection

Legal protections do not cleanly apply to the digital world, and the woes of digital property owners do not end there. Frequently, a legal remedy provides no practical help. Take a legal victory in a criminal case: the remedy is exclusion of the seized and searched evidence at trial. In civil cases, the remedy is monetary compensation. Most digital property owners, however, are not looking for evidentiary exclusion or money; they want barriers to data loss and real privacy protections. Moreover, most violators of digital property rights are often not deterred by the law. If fact, you probably know someone who rampantly ignores digital property ownership.

There are two hurdles that digital property owners face in attempting to reform legal protections. The first is legislative change. To curtail government surveillance programs, the laws that govern the operations of surveillance and law enforcement agencies would have to be amended to restrict their activities or limit their funding. The passage of the USA FREEDOM Act shows that this option is time consuming, subject to political dispute, and delivers imperfect outcomes. The second hurdle is an individual's right of contract. Placing restrictions on terms-of-service agreements for third-party providers could infringe on the service providers' and users' ability to freely enter into contracts.[11] Finally, these reforms do nothing to deter cybercriminals who rampantly ignore the law entirely.

As we move to a more digital world that relies on cloud computing and greater connectedness, we are required to recognize the security vulnerabilities of digital property. This issue is both legal and technological by nature, and conforming current legal paradigms to digital property proves untenable. More proactive protective measures that enhance the security of digital property where traditional legal protections fall short are needed. The legal landscape is ever-changing, and it is likely that a proper legal paradigm will eventually emerge. Until that day comes, however, users should take proactive steps to protect themselves. IT

References

1. J. Wilson, "On the History of Property," 1804.
2. Ghen v. Rich, *Federal Reporter*, vol. 8, 1881, p. 159.
3. Katz v. United States, *US Reports*, vol. 389, 1967, p. 347 (Harlan concurring).

4. Katz v. United States, *US Reports*, vol. 389, 1967, p. 347.
5. US Code, Title 18, sections 2701–2712, 1986, as amended.
6. Ex Parte Jackson, *US Reports*, vol. 96, 1877, p. 727.
7. United States v. Choate, *Federal Reporter*, 2nd Series, vol. 576, 1978, p. 165 (US Court of Appeals for the 9th Circuit).
8. Smith v. Maryland, *US Reports*, vol. 442, 1979, p. 735.
9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Public Law No. 107-56, section 209, *US Statutes at Large*, vol. 115, 2001, p. 285.
10. Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, Public Law No. 114-23, *US Statutes at Large*, vol. 129, 2015, p. 267.
11. *Restatement (Second) of Contracts*, section 187, 1981.

Joseph Webster *is a founder at ShieldMyfiles and a software and systems security architect. He specializes in high-quality secure software systems to protect privacy, valuable assets, and intellectual property. Webster is a passionate advocate for privacy and secure development and testing methodologies to promote best security practices for all. He is a Certified Information Systems Security Professional (CISSP). Contact him at joe@shieldmyfiles.com, or via https://www.linkedin.com/in/josephwebster.*

Max Romanik *is a founder at ShieldMyfiles. His research interests include the intersection of law, technology, and privacy, as well as healthcare technology and security. Romanik received a JD from the University of Maryland School of Law and an MBA from the Robert H. Smith School of Business at the University of Maryland. He is a member of the Maryland State Bar and is a professional member of IEEE. Contact him at max@shieldmyfiles.com or on Twitter @MaxRomanik.*

Christopher Webster *is a founder at ShieldMyfiles. His research interests include digital privacy law and policy, emergency preparedness, and crisis management. Webster received a JD from the University of Maryland School of Law. He is a member of the Maryland State Bar and is a professional member of IEEE. Contact him at chris@shieldmyfiles.com or on Twitter @christophersw1.*