Daniel E. Geer, Jr.
In-Q-Tel

Ownership

Personal responsibility, economic liberty, and the owning of property are how we got to where we are. They are how we get to a future that we can tolerate, indeed enjoy.

In societies without effective property rights, the poor can never escape their poverty—the lack of effective property rights keeps the poor in their place. The question we consider here is what is "effective property rights" and what is "poverty" in the digitalized world. Because no machinery can sit idle indefinitely and be expected to still run when asked, we might ask how long a people who do have these rights can choose not to use them yet still have exercisable rights should they later want to do so.

Which brings us to XYZ-as-a-service business models and the triad of property rights, liberty, and personal responsibility. This being a word-count-limited column for readers of *IEEE Security & Privacy* magazine, let's be crisp.

If you own something, your ownership includes the ineluctable liberty to use the thing you own as you see fit. In addition to my day job in cybersecurity, I run a farm. Every real farmer I've ever met is a repurposer, an experimentalist, a fixer, a modifier, a tinkerer, which is to say a mix of problem solver and inventor. Ditto anyone who does digital forensics. We here in cybersecurity are blood brothers to farmers; see farmhack.org/tools if needing proof by demonstration.

However, and you all know this, we repurposers, experimentalists, fixers, modifiers, tinkerers, are under constant threat of being called a threat exactly because we repurpose, we experiment, we fix, we modify, and/or we tinker. Why is this? Two reasons: 1) We are up against vested interests that do not want us to own our data or our software and have gotten their way about that for something like forever, and 2) laws exist that are just plain wrong about the issues of what begets cybersecurity. Colleague Andrew Burt and I've taken the latter on with respect to the Computer Fraud and Abuse Act (CFAA) ("Flat Light," www.hoover.org/research/flat-light) and with respect to The Budapest Convention on Cybercrime ("Modernizing Crimes in Cyberspace," forthcoming). The short form: intent (*mens rea*) and action (*actus res*) are each necessary to show a cybercrime exists, but most law (CFAA, say) doesn't care about intent, only action. Distinctions that matter, like the difference between murder and justifiable homicide, are all about the intersection of action with intent.

As to the first point 1), the vested interests go in the direction of contract law, which is to say that a licensure construct is their preferred alternative to you actually owning the product lest you were to have the liberty that real ownership is all about. Of course, they don't say this straight away—that would be too easy to counter in the Court of Logic. What they say instead is that repurposing, experimenting, fixing, modifying, and/or tinkering with software is a clear and present danger to civil society. They argue that repurposing, experimenting, fixing, modifying, and/or tinkering with software is something that only knaves, not normal people, would want to do, and that those knaves' actions must all be forbidden in the name of public safety.

Hiding how something works benefits only those who've done the hiding.

Humbug.

Consistent with our historic understanding that obscurity is not security, IEEE's readership knows that hiding how something works benefits only those who've done the hiding, just as we know that the truth of what a system can really do is oft found only by

continued on p. 99

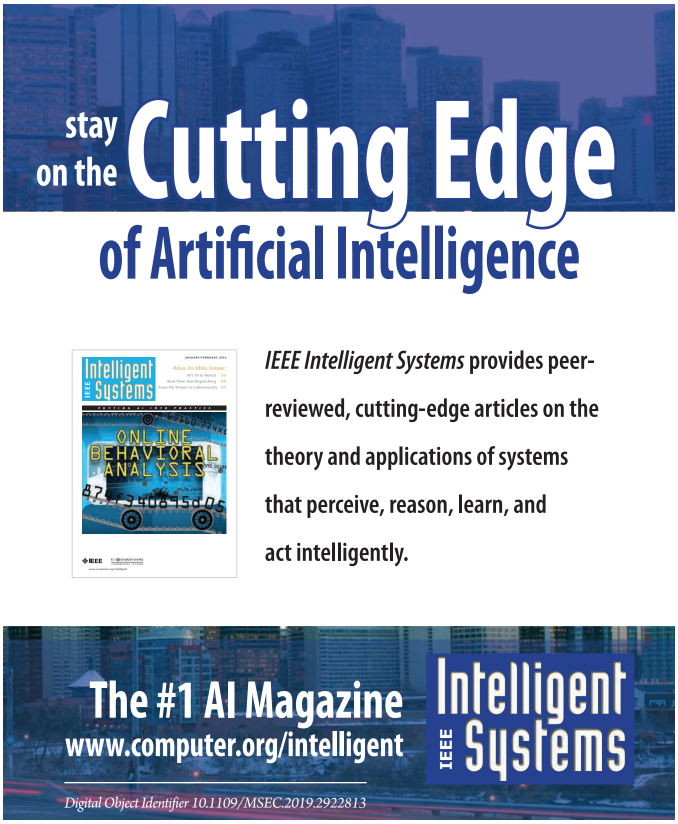
Digital Object Identifier 10.1109/MSEC.2019.2914845
Date of publication: 9 July 2019

continued from p. 100

experiment. We lost the word *hack* to fearmongers when we did not defend the distinction of intent. We cannot lose repurposing, experimenting, fixing, modifying, and/or tinkering because we did not defend effective property rights. A poverty of self-determination awaits if we do nothing.

Which brings us to the point: we have a natural duty to align ourselves with "the right to repair" and the efforts underway in legislatures to affirm that ownership rights, like the right to repair, do apply to the digitalized world, that an impenetrable, interminable end-user license agreement is not the last word on who owns what. The nascent rallying organization securepairs.org is a good start; its statement of principles will resonate with you. We have a duty here; drift is not a strategy. ■

Daniel E. Geer, Jr. is the chief information security officer at In-Q-Tel. Contact him at dan@geer.org.



Digital Object Identifier 10.1109/MSEC.2019.2922813

Digital Object Identifier 10.1109/MSEC.2019.2922814