DC|IA

Distributed Computing Industry Association

A DRM MANIFESTO

2015 CINCO DE MAYO MESSAGE ON DIGITAL RIGHTS MANAGEMENT

For those hoping for a frothy and free-wheeling Cinco de Mayo message, this will surely disappoint.

But for those willing to consider a serious topic and take an open-minded approach, this communiqué could mark a turning point for an oft-maligned industry and provide an opportunity to act meaningfully to benefit all Internet users — and people in general.

Today's date is observed to commemorate the Mexican army's unlikely triumph over French forces at the Battle of Puebla on May 5, 1862. The victory represented a significant morale boost to the people of Mexico.

As noted on The History Channel, "Zaragoza's success at Puebla represented a great symbolic victory for the Mexican government and bolstered the resistance movement."

And as Time Magazine remarked, "The Puebla victory came to symbolize unity and pride for what seemed like a Mexican David defeating a French Goliath."

It helped establish a much-needed sense of national unity and patriotism.

A DAVID VS. GOLIATH MISSION

In that spirit, we seek to commence an era of new industry accord and resolve for those engaged in improving the integrity, security, and value of the Internet for software development, broadband access, data storage, and content delivery; and for consumers and enterprise end-users of web-based services.

For theirs is also a David vs. Goliath mission; and it is one of seriously increasing importance to be encouraged rather than disparaged.

Unlawful attempts to justify digital infringement and disruption are now threatening far more than the economic insult inflicted by the pirating of music tracks or the hacking of company emails.

With the emergence of the Internet of Things (IoT) heralding such advances as connected automobiles and embedded medical devices, seeking to overturn the work of those charged with protecting these data systems can result not only in data loss, but also in serious physical injury or death.

The horrors of a fatal accident as a result of a brake failure caused by compromising and sabotaging a connected car or death as a result of heart failure caused by compromising and sabotaging a connected pacemaker are all too real as we approach mid-year in 2015.

The TSA is now asking airline passengers to be on the lookout for terrorists trying to gain control of planes through in-flight Wi-Fi networks, entertainment systems, or under-seat ports; and the Department of Defense (DoD) would not even consider the deployment of military drones or missiles without encryption.

European Union authorities have projected that the first murder-by-Internet will be committed in 2015.

That this has not yet occurred is a matter more of fortunate circumstance than of effective preparedness.

• DIGITAL RIGHTS MANAGEMENT (DRM) MEANS ACCESS CONTROL

A term-of-art employed to describe a principal area of endeavor performed by those working to prevent these tragedies is Digital Rights Management (DRM), which has been subject to a barrage of misplaced criticism, uninformed disrespect, intentional misunderstanding, and undeserved opposition.

A neutral synonym for DRM is access control. Controlling access is what provides security, protects privacy, and ensures safety for all Internet users; and it is access control precisely that is becoming a life-and-death matter.

At a time when controlling access to Internet communications of all kinds is more critical than ever, misguided opponents of DRM are mounting new assaults.

Without consideration of abatement or attempting resolution of any legitimate concerns, the "Free Software Foundation (FSF)," for example, is attempting to resurrect its "Defective by Design (DbD)" campaign under the subject line "Hate DRM? Tell the World on May 6th."

In the spirit of transparency, yes — the timing of our message to preempt the 2015 DbD by one day is intentional.

MISGUIDED OPPOSITION

Deliberately mischaracterizing DRM as Digital "Restrictions" Management, FSF seeks to incite unlawful behavior by demonizing DRM as instilling an "oppressive effect" and stridently inciting consumers to "fight against DRM" and "regain the control of our technology" on its so-called "International Day Against DRM," which upon even a modicum of reflection is as ill-conceived as it is dangerous.

FSF goes on to mock and condemn the otherwise highly-regarded work of the US Library of Congress (LoC) in granting reasonable exemptions from the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA), accusing the venerated LoC of "doing whatever the heck it wants," smearing its thoughtful and balanced decision-making process as "comically wrong," and applying such euphemisms to lawbreaking infringers as merely "individuals who care about controlling their own computing."

FSF calls "every digital restriction an affront to freedom" and calls for the LoC to "simply end this madness and create an exemption for all uses." In a true black-is-white conflation, FSF wrongfully indicts protecting the integrity of data online as "criminalizing user freedom."

These inflammatory and wrongful exhortations come at a time when even the shadowy FSF must acknowledge that the civilized world is moving in the opposite direction.

FSF itself does so by citing — although in as discrediting a manner as possible — the widely respected Mozilla's adoption of DRM in its popular Firefox web browser through a partnership with major software company Adobe to implement Encrypted Media Extensions (EME).

And also by noting — although again in as deprecating a way as it can — the industry leading Apple's announcements of deploying DRM to ensure the integrity in performance of its new iPhone, Apple Watch, and Apple Pay.

To which we would add that there would be no Netflix without DRM. No Amazon Prime. No Hulu. No Rhapsody. No Spotify. There would be no major motion pictures or premium television programs available on a video-on-demand (VoD) basis or on digital video recorders (DVRs). HBO's planned Internet delivery would not be happening without DRM.

INDUSTRY ACCEPTANCE & ADOPTION

That these technology and media sector leading brands, among many, many others, have fully committed to using DRM is due in good measure to the conduct of DRM industry participants, who are working hard to meet their responsibilities to protect software developers, broadband network operators, end-users, and data rights-holders in effective, economically attractive — and less-and-less intrusive ways.

Encryption, which is a core functionality of DRM, is essential to the development of software that generates and transmits sensitive data for the IoT. There would be no Wi-Fi without access control. Mobile cloud could not develop without encryption. Big data can only be of value if it is also secure data. And social networking would not work without privacy settings that are a function of DRM.

The problem is not that DRM cannot be made perfect. Industry participants accept the existence of the "analog hole" for playback of content for human consumption, which opens up the possibility of re-recording content at that point.

Just as everyone knows that in the physical world, locks can be picked, doors broken down, and walls penetrated; security monitors can be circumvented; guards blocked and police officers impeded from executing their duties to protect people and property.

In many ways, protective systems in civilized societies provide guidelines for law-abiding citizens and delineate, rather than absolutely prevent behaviors that are considered criminal.

But what right-minded person would prefer to live in a world without any such protections?

• POTENTIAL IMPACT ON USERS

The problem is that this year's FSF anti-DRM day does not represent the first time it has attempted to incite reckless, unlawful, and dangerous acts.

And FSF's malfeasance is not isolated to its DbD campaign. It regularly issues factually wrong but disturbingly incendiary public announcements that instigate anarchic behavior and oppose responsible use of the Internet.

As Linux Magazine journalist Joe Brockmeier said, the DbD campaign by the FSF is "negative" and "juvenile," and woefully inadequate because it fails to provide users with "credible alternatives" to proprietary software.

We hope that every reader of this Cinco de Mayo message, regardless of his or her views on this subject, will take time, if not today, then at some other point in the near future, to deeply ponder the real issues at stake here, and carefully consider their potential impact on each one of us.

The irony of confronting this matter on a minor holiday that celebrates accord fostered by an obscure military victory against long odds need not be lost on us; but let us resolve to make the right determination in actions that we take in addressing it.

For at a time when online insecurity, as more and more types of devices add sensors, drivers, switches, and modems and connect to the Internet, continues to be our most crucial concern, the dangers from unauthorized access pose an increased threat, not only to the rights of software developers, network operators, consumers, and content providers, but also to the viability of human activities of every kind, and now even to human lives.

Beside the reasons of poor performance or lack of perceived value, the principal reason that consumers shun a high-technology product or service is that it endangers them.

When a technology ignores, downplays, or fails to protect the fundamental safety of humans, people will wish to distance themselves from that danger; and if the threat is sufficiently severe, to reject the technology.

For many Internet users, both at a personal level and for business use, the escalation of threats to their security, almost by definition, represents such a fundamental violation.

• FREEDOM OF SPEECH & RESPECT FOR RULE OF LAW

The Internet has thrived and advanced, more than in any other nation, in the United States of America (USA), a country based on great human principles, including one that states that all of its citizens are created equal, and that the rights of every citizen are diminished when the rights of one are denied.

And the ideals of digital rights managers are bound in many ways to those of the USA, whose liberties include the proud proclamation of freedom of speech, but whose duties also encompass respect for the rule of law.

DRM providers are sensitive to past criticism regarding inconvenience to legitimate end-users of content delivered over the Internet, and are resolved to ensure that this does not happen going forward.

They deeply appreciate that the worst abuses made DRM as objectionable as malware, and are fully committed to corrective actions so that these do not recur.

However, they are also adamant that translating accepted physical world norms for security -- walls, doors, and locks -- to the virtual world is not only justifiable, it's wholly necessary.

And they are confident that as in the physical world, digital equivalents of monitors and guardians are likewise required to ensure the integrity of a secure online environment.

But DRM providers also proudly acknowledge that they are at their best when they are more than transparent — when they are perceptibly invisible.

• BEYOND TRANSPARENCY -- PERCEPTIBLE INVISIBILITY

When professional software developers sign-up for creating an innovative new application, or for materially improving features in an existing computer program or operating system, they do not sign-up to work in a world where they cannot earn income for their efforts, but neither do they sign-up to work in a world dominated by DRM considerations; they sign-up to receive payments for the value created by their work and the revenue generated from licensing or advertising or other business model.

When broadband network operators sign-up to invest in the infrastructure to improve the access, speed, and reliability of their Internet access services, they do not sign-up for obtrusive DRM technologies to impede such advances; they sign-up to provide their subscribers with more robust and useful services.

When consumers sign-up for entertainment services that use DRM, or access data files or streaming media that is DRM protected, they do not sign-up for the Advanced Access Content System (AACS), Content Scrambling System (CSS), Marlin DRM, Protected Media Path (PMP), or Windows Media DRM; they sign-up to access the content that the DRM system enables.

And when professional content creators and distributors sign-up to devote their time, labor, and talent to producing and marketing motion pictures, television programs, music, or games, neither do they sign-up for an overbearing DRM relationship; they sign-up to receive compensation for their work from their share of the revenue generated by offline and online ticket sales, subscriptions, rentals, and advertising.

These expectations match what these parties hold as fundamental tenets of acceptable behavior in the physical world of a free society when it is working at its best.

• BALANCING ACCESS AND PROTECTION

Commercial pursuit and technological advancement are enabled. Both sides of the property rights equation — access and protection — are honored and protected. And security is omnipresent but unobtrusive.

It ought to be possible, therefore, for software developers to protect their intellectual property (IP) and licensing terms without being confronted with hostility from self-proclaimed advocates of digital freedom like FSF.

It ought to be possible for Internet service providers (ISPs) to safeguard the integrity of their offerings without the condemnation of entities like FSF.

It ought to be possible for consumers to choose content and software that respects the rights of others and protects their own security without confronting antagonism from FSF.

It ought to be possible for data rights-holders to defend their business models and ensure the integrity of their digital content delivery and be treated with tolerance, respect, and civility.

And it ought to be possible for digital rights managers to work to ensure that the lawful intentions, business models, and fundamental security of software programmers, ISPs, end-users, and content providers are protected without being attacked and undermined.

It ought to be possible, in short, for every lawful user of the Internet throughout the distribution chain to receive the benefits of DRM without being subject to ridicule.

These organizations and people ought to have the right to be treated as they wish to be treated, as they wish their colleagues, family members, and associates to be treated.

- **HYPOCRISY OF OPPONENTS**

But this is not the case when the FSF and other ill-advised entities are doing all that they can to foment hate and destruction of DRM.

Its DbD campaign would be excusable if after conducting it, FSF's leaders took reasonable steps to work as responsible adults with digital rights managers to address whatever legitimate issues they have identified.

Denying the opportunity for software developers, network operators, and content creators to earn compensation and jeopardizing the security and safety of consumers, however, are not reasonable expectations for the outcome of such discussions.

The fact that DbD has happened not once, not twice, but nine consecutive times — and not once has FSF ever sought constructive resolution as a follow-up — is just not acceptable in today's world.

And FSF's own hypocrisy need not be ignored. There are locks on the doors at its Franklin Street headquarters in Boston, MA; and its own website requires users to provide a password in order to log into their accounts (https://cas.fsf.org/login) — rather than providing free access to everything.

This is not a problem solely of the FSF, however.

- **INTERNET SECURITY -- A LARGER ISSUE**

Insensitivity regarding online infringement and recklessness with regard to Internet security exists throughout the digital ecosystem, and indeed at every level of human society.

When a parent discovers but ignores the fact that his or her child has acquired a music collection or movie library by accessing a file-sharing system that does not support rights-holder authorization, he or she condones disrespect for the rights of others and embarks down a slippery slope in the direction of thievery, larceny, and worse.

When an organization chooses to ignore the risks of exposing its employees and customers to unprotected data, it signals to the world that it is does not care whether its most important constituents are reasonably protected in the workplace and marketplace.

When the US Congress considers, even for a minute, anarchic proposals like the Apollo 1201 Project, which unabashedly pursues the "eradication of DRM in our lifetime" by dismantling

Section 1201 of the DMCA, it displays a reckless disregard for Internet security and the safety of American citizens.

DMCA's anti-circumvention clause is essential, given the ease with which digital replication and dissemination — including of a DRM breach — now enables access to millions of users instantly by hackers.

The analogy Apollo 1201 organizers choose to make is that DRM is like the scene from the 1968 motion picture "2001: A Space Odyssey" in which a mainframe computer turns on its operator and says, "I can't let you do that, Dave," when in fact, well-implemented DRM would have prevented that from occurring.

It is DRM, with its core components of encryption and authentication that provide Internet users with their best weapons against surveillance, censorship, and monopolistic practices.

If we don't want our offline as well as online future to be as secure as possible, governed by the rule of law and respectful of the rights of all participants, and if we don't want the Internet to be usable in safe and predictable ways, then we can ensure that future by behaving irresponsibly as the FSF and Apollo 1201 Project exponents would provoke us to do.

• CONFRONTING AN AGE-OLD PROBLEM

This should not need to be a matter that requires the heavy hand of federal government intervention.

Well-intentioned measures, such as the recently introduced but not pursued "You Own Devices Act (YODA)," are not necessary to provide the legal authorization to package software, content, and hardware for sale in the consumer marketplace.

The law already provides for such bundling of products and services.

This should not even need to be an operational issue to be addressed by adding a paragraph to users' manuals or end-user license agreements (EULAs). It would be far better to settle this matter through the simple practical adoption of common-sense good behavior.

And while a sense of fair play and understanding and recognition that all users have rights that are equally deserving of protection are clearly needed, a change in attitude alone will not work for all Internet users.

The problems of acceptance and mutual respect among groups of people are as old as civilization and as straightforward as the golden rule: "Do unto others as you would have them do unto you."

The heart of the question is whether all Internet users — software developers, ISPs, consumers, and content providers, are honestly to be afforded an equal opportunity to pursue the legitimate pursuits of their choice and an equal opportunity to have their rights protected in the online world.

- ## DRM ENABLES ADVANCEMENT

The argument that DRM favors large corporations over small entrepreneurs is entirely unfounded.

Just as cloud computing brings enormous storage capabilities and computing power to very modestly funded entities, on a highly affordable basis; so DRM provides them with unprecedented opportunities to protect their software, data, and other digital assets on extremely attractive terms.

The fact is that giant multinationals have many other resources to bring to bear on alleged violations; it is DRM that levels the playing field for the small entrants to enjoy the same protection when they don't have such other major resources available.

It is DRM that enables innovation and competition in the digital world.

If Internet users, who happen to be software developers, cannot trust that licenses for their applications will be honored; if broadband network operators cannot trust their terms of service will be respected, if consumers cannot trust that their security and privacy will be protected; if content providers cannot trust that their works will not be infringed; then who among us should be content to continue indefinitely to use the Internet?

Yet, here we are again on the eve of another "Hate DRM Day." We have not learned to behave online in a civilized manner, to tolerate, understand, accept, and support the rights of all other Internet users. We have not made all users feel equally treated.

And our online communities, with all their claims and all their good intentions, would be hypocritical to say they are respectful of all and not prejudiced against some.

The opponents of DRM talk about equity, openness, and freedom; but are we to say to Internet users in general, and much more importantly, to ourselves, that we simply disregard or disrespect the rights of others when we feel like it; or that since we're only a single individual, the impact of our so doing should be ignored; or that we'll try harder from now on and so everyone should just trust us?

- ## TIME NOW FOR ACTION

It's time to say no to that. The time has come for the Internet to fulfill its promise for all its users with clarity and truth on this very important matter.

The events surrounding DbD and Apollo 1201 and elsewhere this year have brought this issue to the point that no Internet user can prudently choose any longer to ignore it, or kick the problem down the road for future users to address.

The frustration can be felt among software developers, ISPs, consumers, content providers, and digital rights managers, where insensitivity is leading to disenchantment, and where even abandonment of the Internet in favor of closed broadband networks is becoming a consideration.

We face primarily a moral issue. One that cannot be met by procrastination or obfuscation. One that cannot be quieted by token moves or idle talk. It is time finally to act, in our professional activities and, above all, in our daily lives.

At its core, the problem stems from society's advancement to the current information age and the increase in relative value of digital services, intangible goods, and virtual products. IP now must be afforded the same considerations that physical property received in prior eras. It is this change in attitude that has fallen behind.

But not to acknowledge this in today's world is as anachronistic as advocating a return to the stone-age.

It is not acceptable to pin the blame on others, to say not understanding this is a problem of an ill-informed consumer advocacy group, or an irresponsible parent, or thoughtless information technology (IT) department at a company, or misguided Member of Congress.

Or to deplore the fact that we must be the ones who have to address this issue. The time to address it is now; and our task, our obligation, is to accept our responsibility and make transformation positive and constructive for all.

Those who do nothing face increasingly serious threats to their own security. Those who join us are recognizing truth as well as helping to expand the horizon for the Internet.

- ## INDUSTRY-WIDE CHANGE

The FSF may not be prepared to make a commitment that it has not made in nearly a decade of mounting its ill-conceived war on DRM, to the proposition that disregarding the rights of others has no place in acceptable Internet behavior. And we have to accept the fact that the FSF may continue to refuse to seek resolution of whatever legitimate concerns it may have.

But there are modest and practical measures we can take as individuals and in our companies and membership groups, to set an example, and possibly serve as role models for future adoption.

We are, therefore, asking that all Internet users modify their behavior in incremental ways — and set an example for the rest of the world — by explicitly codifying the harmful behaviors we need to prevent at the same time as memorializing the beneficial practices we need to protect, and acting accordingly.

A number of digital rights managers are taking voluntary action to adopt these measures as well. But many are unwilling to act alone, and for this reason, Internet-wide change is needed if we are to address this problem in any real and meaningful way.

- **VOLUNTARY CODE OF CONDUCT**

For prevention:

1. Our policy shall be not to support implementations of DRM that disrespect the rights of Internet users.

2. DRM shall not be unduly restrictive or harmful to any individual's lawful use of the Internet.

3. DRM policies shall not impede Internet users from exercising lawful authorizations to back-up copies of digital content, access public-domain works, use copyrighted materials for research and education, or other permitted usages under fair use-laws.

4. DRM shall not require access to a single-thread authentication system to enable content access.

5. DRM shall not allow unauthorized users to have greater freedom of use or obtain greater utility than authorized users.

These seem to be the core problems, and their elimination should remove arbitrary impositions and privacy intrusions that no Internet user should have to endure. We are also asking individual users and Internet-based companies to underscore the positives.

For protection:

1. Software programs, Internet access services, and content offerings shall accept reasonable DRM technologies, and DRM shall be supported throughout the distribution chain.

2. DRM implementations that increase the value and utility of content shall be encouraged.

3. DRM shall be enabled and shall be forward compatible, guaranteeing that rights granted to end-users will be protected as technology changes.

4. DRM shall be implemented in ways that provide redundancy to ensure continued access to content in case of such incidents as server failure.

5. DRM shall take into account the realities of computer maintenance such as operating system upgrades and hard-drive replacements, and provide user-friendly methods to ensure that end-user rights are respected in all such instances.

These actions will reflect not only our tolerance of the rights of all Internet users, but also our desire to proactively encourage the pursuit of the chosen missions of all users.

And this in turn will lead to a stronger and more robust Internet. For it is a basic tenet of organizational dynamics that the strength of any group is a function of the degree to which it can leverage the differences of its members, enabling them to address more complex problems than otherwise, by using a diversity of methods.

- ## A BETTER FUTURE

Beyond that, we are on the side of advocating freedom in Internet activities, of benefiting from the multiplicity of opinions and advantages that are brought forth through free speech. Fostering the sense of community and good will towards other Internet users is at the center of our initiative.

Other features may also be requested, including additional preventive and additional protective measures, and the implementation of these voluntary changes shall not be left to chance.

But such efforts led by the actions of digital rights managers, we repeat, cannot solve this problem alone. It must be solved in the homes and in the cars and on the mobile devices of every individual and in the offices and in the factories and on the servers of every institutional user.

In this respect we want to pay tribute to those consumers who have subscribed to services with DRM. They have been acting with basic moral consideration for right and wrong and respecting the rights of others.

Like the most enlightened digital rights managers throughout the digital ecosystem, they are meeting the challenge of Internet security on the front line, and we salute them for their good character.

We are also asking for your help in making it easier for us to move ahead and to provide the kind of equality of treatment that truly reflects the best of who we are; to give a chance for every Internet user to be comfortable in the fact that his or her rights will be fully respected online.

We should be able to expect that other Internet users will be reasonable and they should expect that our conduct will be fair.

We have a rare opportunity to make the online world a better place than the physical world — and we should take it.

With sincere best wishes for a happy, healthy, mutually respectful, and possibly even memorable Cinco de Mayo.

Signatories:

Advancement of Digital Rights Management (ADRM) Working Group

BuyDRM

Distributed Computing Industry Association (DCIA)

Genos Corporation