Custos for eBooks
Frequently Asked Questions

General

- **How are you different to traditional DRM or watermarking?**

  Hard DRM restricts access to content. The problem with hard DRM is that it affects legitimate consumers by restricting fair-use, while not deterring pirates (hard DRM can often be cracked as various applications for removing it exist). Traditional watermarking with a dumb-watermark is effective at connecting a leaked copy to an infringer – but only once the pirated copy can be found. Pirated content typically circulates in closed social networks or the dark net before reaching a site where a web crawler can find it.

  Our technology does not restrict access (although it can work in combination with hard DRM) and detects piracy wherever it happens. We have had successful detections on closed university networks, social networks, and even in emails.

  Traditional attacks on piracy tries to attack the piracy ecosystem from outside. The piracy ecosystem can be defined as "anti-fragile" – like a muscle, it gets stronger from stress. Attacks from the outside lead to the piracy ecosystem reacting and making itself more robust. Our technology attacks piracy from the inside, using pirates to catch other pirates. This circumvents the antifragility. Please see the Custos whitepaper on the topic.

- **Is a specific app or platform required for the end recipient or reader?**

  No, this is one of the main advantages of our system in that the eBooks we protect conform with open standards e.g. ePub and therefore can be viewed with any compatible reading application. The CustosTech protection is built into the eBook itself, so it remains protected, even if the book is moved between readers.

- **The free extraction tool – where is it available?**

  The online extractor is at http://extract.privateer.xyz/. The downloadable tool will be released later on the Privateer website.

- **Who are your bounty hunters and what kind of coverage do you have?**

  We have a multi-layered approach to bounty hunting. The first line of defence is the network of bounty hunters which have been recruited from all over the world. We like to target college-age tech-savvy individuals, who are frequently already present in piracy communities. These individuals are long on time and short on cash therefore the bounties serve as an effective incentive for finding and reporting infringements. We also have trusted partners who assist us in finding any content that slips through the cracks along with in-house crawlers and a research team constantly analysing pirate communities.

- **How long on average does it take to find a compromised copy?**

  Once a bounty hunter finds the copy, it takes mere seconds for the bounty to be claimed and the system to pick up the infringement. We've run in-house tests with creative commons content, and experienced detections in as little as 30 and 45 seconds on social media platforms and dark networks.

- **Is it safe to use Bitcoin?**

  The Custos team is comprised of engineers and economists specialising in cryptocurrency. They take the responsibility for managing the Bitcoin. As a client, you will never interact with the Bitcoin directly and are not exposed to any volatility of the currency. The Bitcoin and blockchain forms a part of the backend of the technology.

- **Why do you use Bitcoin rather than fiat currency or vouchers?**

  The solution is a global approach to a global problem. Both fiat currency and vouchers are territorially limited. Bitcoin is global – you can have students in India hunting for your French textbooks. Bitcoin also allows the bounty hunters to remain anonymous, which is critical to infiltrating deep piracy networks.

- **Can other cryptocurrency be used?**

  Yes, any blockchain-based cryptocurrency can theoretically be used. Bitcoin is used because the infrastructure and trading volume is far greater than any of the other currencies.

Enforcement

- **Is there any way that someone who is identified as having uploaded an eBook because it has their watermark on it can appeal?**

  We acknowledge that content could be leaked without any malicious intent on the part of the recipient. It should be stressed that it is the responsibility of the recipient to protect their content. We hope the addition of the Custos watermark will induce a sense of responsibility to the recipients of media. That being said, users whose computers are hacked or stolen could appeal any infringement against their name, but as with credit card fraud, the onus will be on them to prove their innocence.

- **Does it matter where a bounty hunter finds a file?**

  No, when a detection is made, it does not point to a source, only to the infringement. While we do not immediately know where the copy of the file was found, it allows our clients to start mitigating damage. We have an in-house team of researchers and advanced web crawling tools to help us find the content as a follow-up to an infringement.

- **What action can the distributor or publisher take when alerted about a found file?**

  This is completely up to the distributor or publisher, but we do advise our clients on the options available to them. If the client chooses to prosecute, we have good relationships with organizations worldwide that can help them with that. Whether they decide to prosecute or not, there are steps that can be taken to mitigate damage from a leak - especially a galley or early release leak.

  In the longer term, we'd like to see industry shifting from a binary "Guilty / Not Guilty" view of piracy, to rather quantifying the risk of potential loss for each individual recipient, and to managing that risk flexibly. The vast majority of honest readers deserve DRM-free content, and we'd like to help our clients recognise these low-risk recipients that are in good standing. Even for higher-risk recipients, prosecution may not always be the best option – for example, a publisher may not want to prosecute a prominent journalist who "lost" an advanced review copy of a book. But knowing who these high-risk individuals are is immensely useful in managing the risks inherent in distributing digital content.

- **What is the point of the bounty?**
  It doesn't physically stop the file from being pirated or make the book unreadable, rather it allows for detection and identification of where the infringement occurred. This tackles piracy at the source and serves as a disincentive rather than a technical barrier. Admittedly some publishers will not find this sufficient and will want the act of copying to be stopped altogether but we know that this isn't necessarily feasible. Many publishers (especially in markets like Germany) are looking into dropping this form of hard-DRM altogether and our solution aims to make this decision easier for them.
  The benefit to the publisher of having the bounty claimed is that it identifies the transaction that lead to the original file being pirated.

Technical

- **What formats are supported?**

  Currently ePub but KF8, mobi and PDF are to be added in the near future.

- **Does the watermark withstand conversions?**

  The watermarking scheme does survive conversions with tools such as Calibre. Our approach here is the same as that for the film industry. Instead of trying to add a watermark that is 100% robust, which is impossible, we add layered forensic watermarks using different schemes, only some of which the extraction tool can detect. The principle is here that a pirate could never be confident that all the levels of the watermark have been removed, and will therefore always be at risk.

- **How are you securing your "free extraction tool" to prevent it being reverse engineered to help hack the watermark?**

  The online tool doesn't readily lend itself to reverse engineering. For the downloadable tool, we use a combination of binary hardening, rotation of "embedding vectors" (ways in which watermarks can be woven into the eBook), and "subset extraction" (the extraction tool does not necessarily expose all available watermarks). This places great risk on a would-be attacker: Even if a current version of the extraction tool fails at reading an attacked eBook, incriminating information is likely to remain, and future versions of the extraction tool (or our own forensic team) may still be able to discover the original infringer's identity.

  This illustrates another advantage of watermarking over "hard DRM". With traditional DRM, in many instances only one successful attack is needed to break the system, e.g. by creating a non-compliant reader that does not honour the scheme. With identity-based watermarks, the embedding approach can be shifted and varied per individual copy, making it very difficult to attack consistently, and imposing a much larger risk on infringers.

- **Are there any techniques you're using to help make the watermark hard to find and strip, given that any e-book watermark can be found and stripped somehow?**

  Yes, please see above. Furthermore, watermarks can continuously be varied to make attacks on the system a constant moving target

- **Does the watermark contain any information about users?**

  The embedded watermark contains no information that can be used to directly identify the recipient by an external third-party. Only Custos can do this once the bounty is claimed.

Business

- **What is the platform likely to be used for?**
    - ARC / Galley copies and promotional copies e.g. to fan clubs
    - Online eBook retail
    - Direct distribution e.g. bulk distribution and B2B
- **Who are your targeting as potential users for the technology?**
    - Distributors as an additional protection option or alternative to hard DRM
    - Watermarking solutions providers as an additional layer of protection and improved detection capability
    - Publishers for business applications listed above (including direct sales)
    - Retailers as an additional protection option or alternative to hard DRM
- **Pricing model – how do you charge for your service?**

  Initial set-up fees depend on client requirements and how the system is being integrated and used. If custom development or integration work is required, then the cost of this is dependent on the level of effort involved.

  Ongoing usage fees are volume based i.e. a charge per publication watermarked with volume discounts available for higher usage levels.
- **How big are the bounties?**

  This varies with the use-case. Ideally the bounties should be large enough to incentivize bounty hunters to actively look for infringed content (a few dollars may be enough to encourage reasonably fast discovery) but shouldn't be so large as to create an incentive for the original recipient to claim the bounty themselves (i.e. the disadvantages of being identified as a source of leaked content should far outweigh the value of the bounty). Typical bounties are $5-$20, but it is technically possible to embed arbitrarily large bounties.
- **Can I embed a client deposit as a bounty?**

  Absolutely, that is one of the use cases. For example, a subcontractor or early access recipient can pay a security deposit for access to the media. This deposit can be directly embedded into the media, and the recipient loses the deposit if the media is leaked. Custos can extract and refund the deposit after a predetermined window period.
- **Is the size of bounties fixed?**

  No, the bounty in a particular media item can be changed over time. For example, a large bounty can be present prior to the official release of the media, after which it drops to a smaller value, and it can be completely removed or deactivated when monitoring is no longer needed.

Where is it currently used?

- **Where is the technology currently being used in other industries?**

  Custos has products in the market in the films industry for both screener and OTT protection.
- **Where is it used for eBooks?**

  Examples of direct sales website which use this technology to protect eBooks can be viewed at www.practisingthepiano.com and https://dfp.informance.biz/ebooks/products.