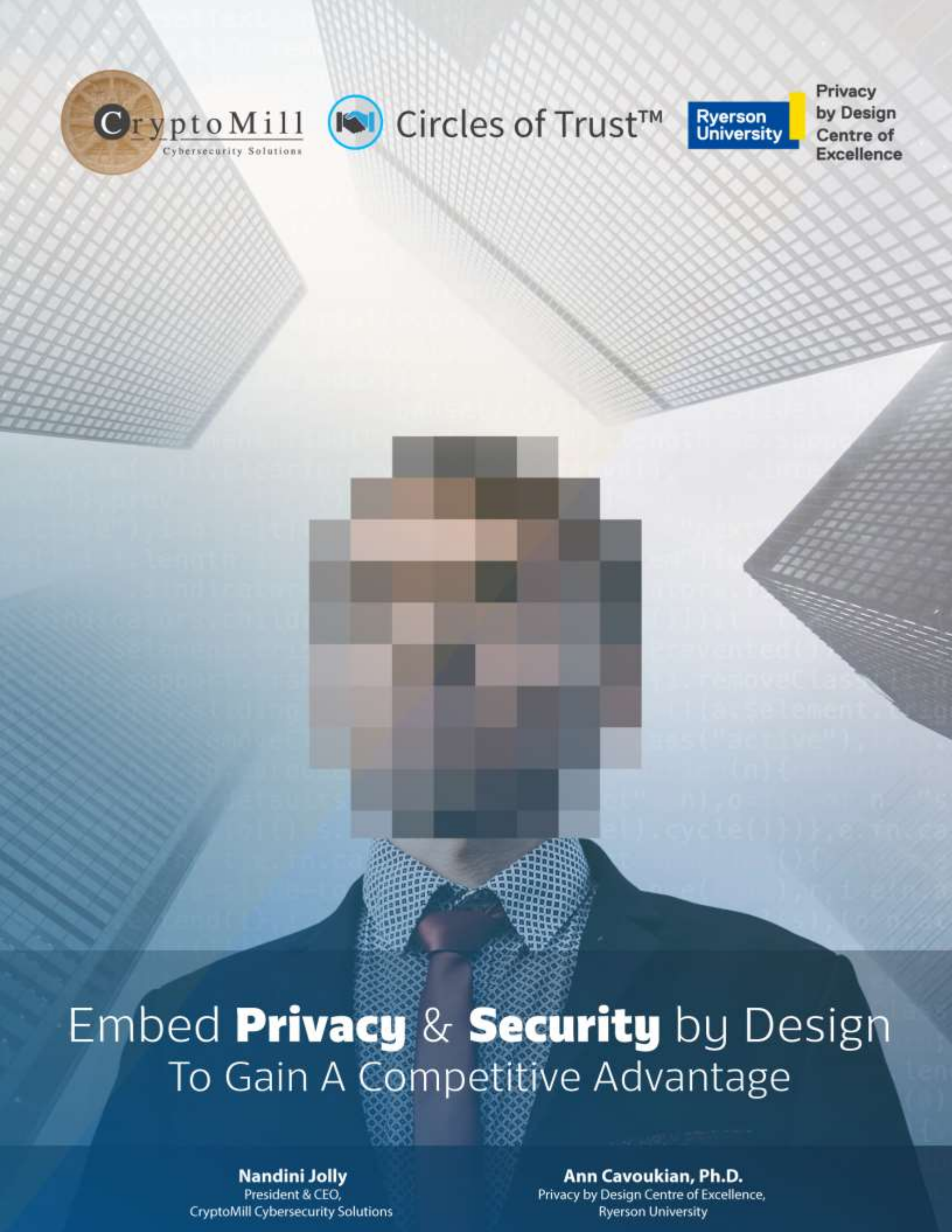
CryptoMill
Cybersecurity Solutions

Circles of Trust™

Ryerson University
Privacy by Design Centre of Excellence



Embed **Privacy** & **Security** by Design
To Gain A Competitive Advantage

Nandini Jolly
President & CEO,
CryptoMill Cybersecurity Solutions

Ann Cavoukian, Ph.D.
Privacy by Design Centre of Excellence,
Ryerson University

Table of Contents

Embed Privacy and Security, by Design to Gain a Competitive Advantage: Circles of Trust™

"The shift to a fundamentally digital economy means that, regardless of the sector you are in, your ability to protect individuals will distinguish your company from competitors who have taken a passive approach or who ignore their responsibilities." David Hoffman, Associate General Counsel and Global Privacy Officer at Intel Corporation, Harvard Business Review (2014)

Overview

As the World Economic Forum (2011) project on "Rethinking Personal Data" noted, "The rapid rate of technological change and commercialization in using personal data is undermining end user confidence and trust. Tensions are rising. Concerns about the misuse of personal data continue to grow. Also mounting is a general public unease about what "they" know about us. Fundamental questions about privacy, property, global governance, human rights – essentially around who should benefit from the products and services built upon personal data – are major uncertainties shaping the opportunity. Yet, we can't just hit the "pause button" and let these issues sort themselves out. Building the legal, cultural, technological and economic infrastructure to enable the development of a balanced personal data ecosystem is vitally important to improving the state of the world." In other words, it is paramount that personal data be protected by default (automatically) wherever and however it travels or resides – in a mobile device, in a corporate database, or in the Cloud – there should be no gaps in protection or accountability for secure storage or transmission. Assuring full lifecycle protection is a significant challenge for organizations today as a result of their operations having become more data-intensive, network dependent, and more accessible than ever before. As data processing technologies, business practices, and networked architectures become more complex and critical for operations, it is essential that security risks are anticipated as early as possible, mitigated by building strong technical and administrative security practices directly in the architecture, as a way of doing business, by default.

Creating Trust in a Digital World

There has been a significant shift in approach to cybersecurity, largely driven by the huge proliferation of endpoints, mobile phones, tablets, laptops, the Internet of Things. This has made the traditional concept of cybersecurity, to create the strongest digital perimeter possible around your institution and put all your important items inside it, no longer practical. People are recognizing that data moves, and the notion that you can put a big wall around it is falling by the wayside. There is an appreciation and acceptance that if we want privacy, security has to travel with the data.

Risk is not always about the potential for loss. It can also create the potential for opportunity. Companies that know how to keep their customer data safe and protect their networks, also understand that cybersecurity can serve as a business enabler. In an increasingly volatile environment where cybercrime seems epidemic, a positive reputation for security becomes a very valuable commodity. Cybersecurity is widely considered to be a cost of doing business, for good reason. Data breaches can devastate both a company's reputation as well as its bottom line. Companies should look to integrating cybersecurity, privacy and digital ethics, right from the outset. This enables them to better engage with existing customers, as well as attracting new ones.

Organizations are gradually beginning to explore how to create value and gain a competitive advantage by integrating information security and privacy with their business strategy. (PwC 2016). With the rising power and influence of the Chief Information Officer, information would appear to be becoming just as valuable as the money managed by the Chief Financial Officer; so protecting that information is essential to gaining a competitive advantage. To be a savvy competitor, firms should be as protective of their innovations and ideas, as they are of their financials. Even cyber-aware organizations can be unfamiliar with the extent to which good cybersecurity can be good for business. Concerns

over risk and cost too often prevail over recognizing how good cybersecurity can be a source of comparative advantage, a product differentiator, a brand asset, and a business opportunity.

Importance of Privacy from a Personal Perspective

Preserving our privacy helps us essentially be ourselves without constant worry of appearing "on a list". Having no fear of searching, reading, learning, talking about any given subject. If we begin to question our fundamental rights, freedom of speech, association, etc., we then begin to question exercising them, as we feel every little action we make, may put us on a watch list. Then we begin the path to losing our freedom. We need to be able to live our lives without constantly gazing over our shoulders looking for cameras, thinking everything we say or write is being heard, read, analyzed, reported and stored.

Consider going home after a work day, but knowing that in your TV is a camera pointed at you, following wherever you go, watching and noting your every move. This is straight out of George Orwell's novel *1984*, perhaps an extreme example, but it demonstrates how easily our privacy may be eroded.

Privacy is something we value every day. We have our own rooms growing up, we say things like "None of your business" to avoid questions, whether we realize it or not. Sometimes it is taken for granted. *"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say" – Edward Snowden.*

Privacy is not about secrecy – it's all about control: personal control over the uses and of our personal information.

Importance of Privacy from a Corporate Perspective

More and more customers are now aware of the threats to their privacy and are growing increasingly concerned about what information is being collected and by whom, where it is going, etc. What's being collected, who is collecting it, where is it going, etc. This fear is realistic and rational.

Having proper security functions and features allows for companies to build better relationships with customers, carry the data safer, and create better branding for themselves. Privacy and incorporated security can significantly help companies gain a competitive advantage over their competitors. *We see companies that are saying, I can use this as a competitive advantage, because if you can trust me more than you can trust a competitor, perhaps you'll come to me more often." Carolyn Holcomb, CPA.*

If companies can integrate security and privacy into their infrastructure, then they can genuinely say they have both security & privacy built-in to protect and manage user data. This can mitigate customer fears and offer comfort to clients. This also helps build brand image, as a company who values security in a world that there is a general belief that the NSA is spying on everyone.

The caveat for all of this is that if a company makes promises of this importance to its customers, it must be willing to uphold those promises at any cost. Making promises to keep security together, but later being caught in a scandal leaking personal information will be nothing short of catastrophic to a company's branding and image. This is why privacy is incredibly important. For companies, maintaining and protecting that data is critical, especially with all the possibilities of leaks, hacks, attacks, malware and ransomware. There are also numerous guidelines and obligations laid out by government bodies, to ensure that companies have underlying privacy principles built into their systems.

General Data Protection Regulation

With the new General Data Protection Regulation (GDPR) coming into effect in May of 2018, a new set of rules and regulations are set to be enforced, including the necessity to implement *Privacy by Design* in a company's infrastructure. Having pre-existing security measures or, implementing them immediately, will help to prepare companies for the upcoming GDPR. Having faulty security and allowing breaches and hacks to take place can, not only destroy a company's image, but also leave them vulnerable to millions of dollars in fines by the government. Fines within the GDPR are high: the greater of $20 million euros or 4% of annual global turnover. If a company has pre-existing security policies implemented, they may be subject to more lenient rules under the GDPR, especially with encrypted data. For example: if data is breached, the company has an obligation in most instances, to notify users of this occurrence. If the data is encrypted however, they may not need to, as the data will be largely inaccessible to the perpetrators.

Unfortunately, one reason larger companies elect not to implement security early on is, due to the added complexity and cost of doing so, thus leaving them much more vulnerable to attacks. Companies must realize that implementing privacy enhancements will not only be legally required, but will be well worth it in the long run, as they will help to boost image, data safety, and make working with government regulations far easier.

Emerging Technologies & Privacy

In an era of connected technologies and devices, the quality and safety of digital services is key. Cybersecurity practices are evolving. We all recognize that current technologies may impact privacy, but may also contribute to mitigating undesirable effects. Harnessing emerging technologies could provide a solution.

Technology – a double-edged sword

Whereas technology is typically seen as the *cause* of privacy problems, there are also several ways in which information technology can help to solve these problems. There are rules, guidelines and best practices that can be used for designing privacy-preserving systems. Such possibilities range from ethically-informed design methodologies to using encryption to protect personal information from unauthorized use. The 'Privacy by Design' approach, as advocated by Cavoukian (2009) and others, can be regarded as a value sensitive design approach that specifically focuses on privacy. Privacy by Design is a globally recognized framework consisting of 7 Foundational Principles for designing privacy-preserving systems. These principles have at their core that "data protection needs to be viewed in proactive terms rather than being reactive, making privacy by design preventive and not simply remedial" (Cavoukian 2010). Privacy by Design's main point is that data protection should be central in all phases of product life cycles, from initial design to operational use and destruction.

There are emerging technologies that exist today, addressing concerns over privacy, protecting data that builds businesses, bringing simplicity into the most complex environments and having a profound impact. One such technology is CryptoMill's Circles of Trust™. In contrast to standalone encryption schemes, the concept of a Circle of Trust provides the means of enforcing access rights and improving data loss prevention through strong encryption within otherwise high personal data availability environments. "Smart" encryption is one of the most important technologies that can and must be deployed in this fast-changing world of personal data proliferation. Circles of Trust™ provides an excellent example of embedding privacy and security directly into a system.

CryptoMill Circles of Trust™

Circles of Trust™ – CryptoMill's Data Security Platform aims to simplify and attain scale in enterprises, hybrid and mixed cloud environments, efficiently and with minimal disruption, while also accessible to small to medium sized companies cost -effectively. A high performance data security platform, Circles helps companies big and small, move confidently and quickly. Advanced transparent encryption, powerful access controls and a lightweight centralized key management, lets organization encrypt everything. With a seamless and scalable platform using technology, this is an effective way to protect data wherever it resides- any file, repository, and application in any server environment.

The Circles of Trust™ cybersecurity suite, ensures that the sensitive data itself is protected. With Circles, encrypted assets remain protected both at rest and regardless of where they travel, only allowing authorized people to access them, anywhere, everywhere. Encryption is applied automatically, both on data at rest and any time sensitive assets are shared. Security travels with the data and access to encrypted data can be revoked at any time. Circles facilitates secure sharing and collaboration with trusted parties on a need- to- know basis.

Circles' underlying technology, cryptographically binds data to a select group of users and devices, combining file level encryption with convenient, intuitive digital rights management (DRM) capabilities. Once protected, the assets can be used and shared only by members of the Circle. If a protected asset ends up in the wrong hands (a non-member), it stays protected and cannot be decrypted. Circles of Trust™ protects all file formats, videos, images, supports multiple device sync, offers mobile applications, and brings protection to any cloud storage. Circles also protects all sensitive assets stored on a server. Unlike traditional data at rest protection, these assets are protected while the server is operating and active. This provides true, realistic data-at-rest protection against today's most serious threats. Circles of Trust™ eliminates the risks associated with data breaches from a hacker attack on firewall, network, cloud, or emails as well as data leaks through lost or stolen devices.

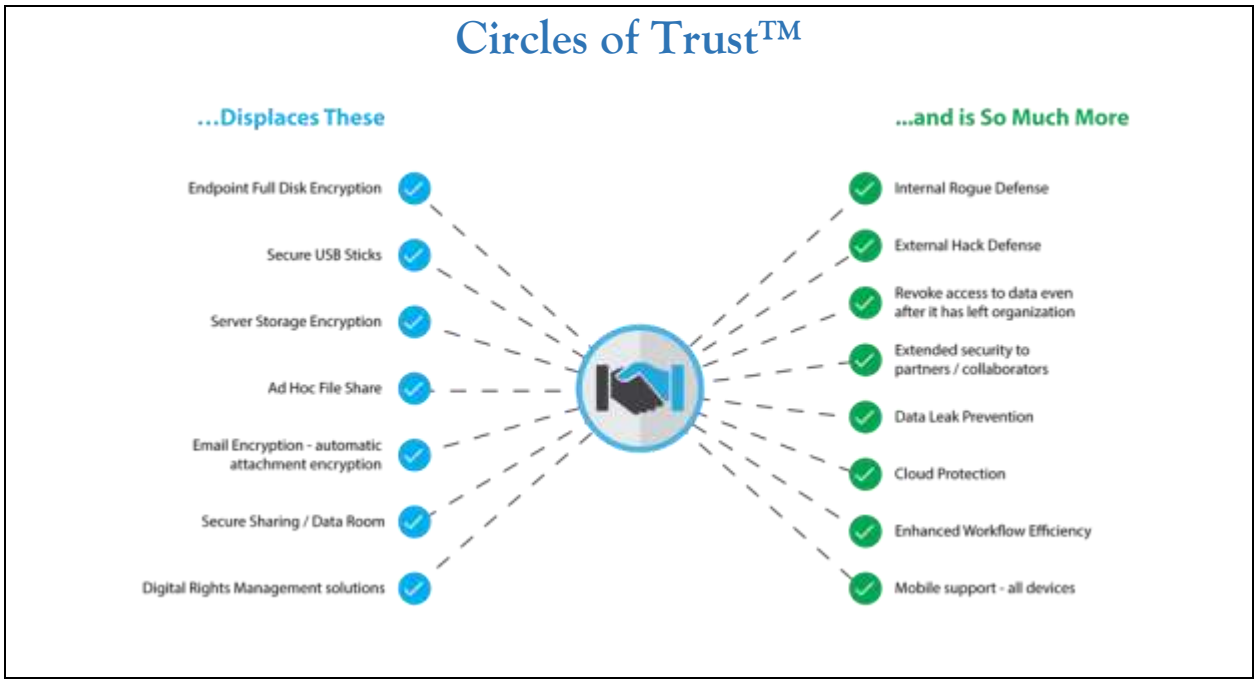


Figure 1 – Circles of Trust™ Features

Protect Data and Preserve Privacy

Circles of Trust™ empowers an organization to create secure groups, or "**Circles**", for sharing and collaboration. These Circles can be defined by a user, by existing organizational structure (e.g. Active Directory), or through automation based on business processes via a rich set of REST APIs.

Files are encrypted in such a way that they can be accessed only by the members of a given Circle. New members can be invited into the Circle based on policy; these members will then be able to access files protected by that Circle. Circle members are not limited to the users within the organization. Membership can be extended to people outside of the organization. This facilitates secure sharing and collaboration, while preserving the integrity of the assets.

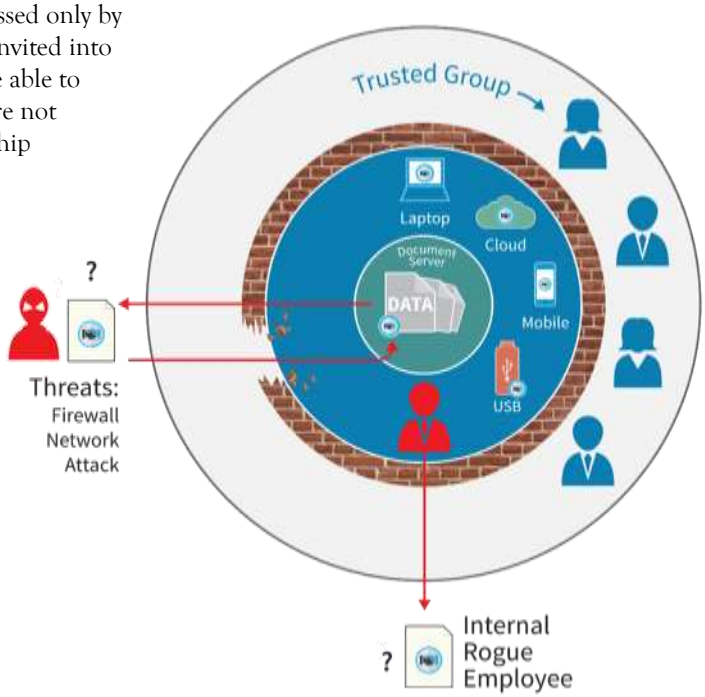


Figure 2 - Threats addressed

Strong granular protection

CoT employs file level encryption to protect each file. Files are protected using AES-256 cipher and each one has its own unique key. All file formats can be encrypted using CoT. The encryption travels with the file such that even if it is copied or moved to a different location or device, it remains protected.

Prevent data leakage

CoT eliminates leaks from a number of different threat vectors. If a hacker breaks into the organization's network or anywhere sensitive files travel (e.g. cloud), they simply cannot get access to the data because they don't have the cryptographic key to decrypt the file. The files are always encrypted on a user's device storage, so that in the event of the device being lost or stolen, the contents of the files are inaccessible.

Any attempts to share data with an unauthorized party (either intentionally or accidentally) will fail since they are not a trusted member of the Circle and hence cannot access the contents of the received files. Even a rogue admin, with physical access to the machines storing sensitive files, cannot gain access to their contents.

Securely accessible anywhere, everywhere

CoT supports all platforms – client software is available for Windows and Mac.
For accessing encrypted data on the go, mobile apps are available for Android and iOS.
Different types of clients are available based on desired use and permissions:

- Trust Edit - a full client install that allows for edit / collaborate capabilities.
- Trust View - a downloadable app that doesn't require installation and provides a view-only sandbox environment.
- Web View - a web application that the user can browse to and view files with no installation, no plugins and no executables to run.

Control over shared assets

CoT enables the organization to have control over their sensitive assets even when they have been shared outside of the organizational border. The organization can limit what levels of access are available to the recipient (Trust Edit / Trust View / Web View). CoT provides capabilities such as: view only, no print, no forward, no copy, no screen-capture. This can be applied at file, member or Circle level. Access can be revoked at any time; even files already downloaded locally will become unreadable.

Similarly, automatic expiry can be set by the organization at multiple levels: file, member or Circle. Once expired, the protected data becomes inaccessible. At end of lifecycle, the data can be securely deleted (through disposal of the cryptographic key), ensuring that nobody can recover access to those encrypted files.

Seamless user workflow

Authorized users have seamless access to CoT encrypted files. At no point does a trusted user need to enter additional passwords nor decrypt the file to be able to access the data. Files are automatically decrypted / encrypted when an authorized user requests access. No plugins are required to work with CoT protected files because the encryption functions independently of the application used to open it. The architecture supports offline functionality - Trust Edit is fully functional offline. This is time limited and tunable based on the organizational policy. (Note that Trust View and Web View require an internet connection).

On-Premise Solution

Circles architecture is based on the premise that the organization has sole and total control over its data and cryptographic keys. This preserves privacy and ensures that recovery is only in the hands of the organization.
CoT captures a host of detailed audit logs relating to:

- User activities - login, logout, failed login attempts, password resets, etc.
- Circle events - create, delete, modify, etc.
- File operations - copy, move, delete, rename, etc.

Administrator roles can be segregated at different levels: full system admin, Circle / policy admin, Circle manager. At no point can an admin add themselves into a Circle in order to obtain illegitimate access to sensitive data.

7 Foundational Principles of Privacy by Design: Applied to Circles of Trust™

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

States that privacy comes at the beginning, doesn't wait for a data breach.
All files within a Circle of Trust are automatically encrypted at the time of creation, ensuring all valuable

assets are protected. Assets remain encrypted throughout their entire lifecycle, thus proactively preventing data leaks by any and all unauthorized parties.

2. Privacy as the *Default Setting*

We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

All data must be secure & encrypted by default, no choice on which ones to encrypt.

Circles of Trust™ can be directly inserted into existing business process workflow such that it automatically encrypts sensitive files as they are created. The encryption is applied by default to sensitive files without the need for any user intervention.

3. Privacy *Embedded* into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Privacy must be held up and embedded throughout the systems design, maintaining a high standard of protection.

Circles of Trust™ is built on CryptoMill's core values of maintaining customer privacy. No sensitive information ever travels through CryptoMill servers, encrypted or otherwise. Access to Circle encryption keys is federated by the on-premises Key Management Server, ensuring that control over access, recovery, and revocation lies solely in the hands of the customer.

4. Full Functionality – *Positive-Sum,* not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

Must be able to have both privacy and security – have everything all in one package.

Circle of Trust's structure and design does not sacrifice privacy for security, or vice versa. Both are upheld as key components throughout the system. This is evidenced by the constant encryption of all Circle documents, and the strong security and privileges that ensure no unwanted guests can access any sensitive data.

5. End-to-End Security – *Full Lifecycle Protection*

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

A piece of personal data is protected throughout its entire lifecycle in the system, and may be destroyed upon completion of its purpose.

Once a file has been protected by a Circle, the underlying data is always fully encrypted. Files remain encrypted as they are viewed, edited, and shared through any means. Even if a file gets stolen, its contents remain fully encrypted, thus preventing any breach of the underlying sensitive data. At the end of the data's lifecycle it can be securely erased through the disposal of the cryptographic keys required to access it; ensuring that no one will ever be able to recover the sensitive data contained therein.

6. Visibility and Transparency – Keep It Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

Maintain a level of transparency to the user of what processes are being applied to the data and how/where it is being used.

The data protection provided by Circles of Trust™ is always plainly visible. Through clear, distinct overlay-icon depiction, the user is always aware of the protection state of a file – be it encrypted, view-only, or in the clear (decrypted). When Circles of Trust™ changes the encryption state of a document, it notifies the user through the standard pop-up notification mechanism. Through the intuitive user interface, it is clear how to change document settings or undo them. In Windows Explorer, all the protection attributes pertaining to a file are readily available via a right-click file properties tab.

7. *Respect* for User Privacy – Keep It *User-Centric*

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Ensure the system is user-friendly and has all the functions to fully operate a Privacy by Design compliant system.

Circles of Trust™ is designed and built to be simple to use and intuitive for individuals. The priorities of the individual come first with Circle of Trust's fluid and seamless user experience. The application's user-friendly design provide s easily-understood security options for both creating and managing Circles. A Circle owner has options to promote, demote and revoke any user, as well as a variety of file control privileges. As part of this user-centric experience, the Circle owner has the ability to easily dictate who has the ability to edit, and who can simply view protected documents.

Biography

Ann Cavoukian

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She is presently the Distinguished Expert-in-Residence, leading the Privacy by Design Centre of Excellence at Ryerson University. Dr. Cavoukian served an unprecedented three terms as the Information & Privacy Commissioner of Ontario, Canada. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible. In 2010, International Privacy Regulators unanimously passed a Resolution recognizing Privacy by Design as an international standard. Since then, PbD has been translated into 40 languages. Dr. Cavoukian has received numerous awards recognizing her leadership in privacy, including being named as one of the *Top 25 Women of Influence in Canada*, named among the *Top 10 Women in Data Security and Privacy*, named as one of the *'Power 50'* by Canadian Business, named as one of the *Top 100 Leaders in Identity*, and most recently, Dr. Cavoukian was awarded the *Meritorious Service Medal* for her outstanding work on creating Privacy by Design and taking it global (May, 2017).

Nandini Jolly

Nandini Jolly is the Founder, President & CEO of CryptoMill Cybersecurity Solutions. Nandini's mantra is security with usability and keeping it simple. In 2013, Nandini was named as one of Canada's 100 Most Powerful Women. In October 2014, Nandini was featured by the Government of Canada's Status of Women Canada. She is a Privacy by Design Ambassador, and co-authored a white paper in 2015 with Dr. Ann Cavoukian when she was Information and Privacy Commissioner of Ontario -"Encryption by Default and Circles of Trust™". Prior to founding CryptoMill, Nandini served as Senior Vice President, Global Treasury Services, Bank of America as well as Director at Deloitte and Touche, National Financial Services Industry Group. CryptoMill's Data Security Platform products aim to simplify and attain scale in large enterprises, and hybrid and mixed cloud environments, with minimal disruption, while also accessible to small to medium sized companies cost effectively. CryptoMill security software suites offer an effective way to protect data wherever it resides—any files and application in any server environment. Persistent, transparent encryption, powerful access controls and a lightweight centralized key management, lets organizations encrypt anywhere, everywhere.

References

Selected Information Resources

Creating Trust in a Digital World

- Fortune Finance Article: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/
- PwC cybersecurity report: http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

Importance of Privacy from a Personal Perspective

- ABC news posted: http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626

Privacy by Design

- Cavoukian, Ann. Creation of a Global Privacy Standard. IPC, November 8, 2006. http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf
- Cavoukian, Ann. 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. IPC, May 2010. http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf
- Cavoukian, Ann. Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. IPC, December 2012. http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf
- For more papers on Privacy by Design refer to: http://www.ryerson.ca/pbdce/papers/

General Data Protection Regulation

- Final text of the GDPR Article 25 https://gdpr-info.eu/art-25-gdpr/

Hoffman, David. Privacy is a Business Opportunity. Harvard Business Review, April 18, 2014. https://hbr.org/2014/04/privacy-is-a-business-opportunity