Cybersafety by Design

7 Fundamental Principles that Use Technology to Protect People Online

mobile | web | devices | wearable | cloud | social | gaming | collaboration | appliances | search | advertising | sharing

Claudiu Popa CIPP CISA CISSP
Founder, KnowledgeFlow.ca
CEO, Informatica

Table of Contents

Introduction 3

The 7 Principles of Cybersafety by Design 5

A Platform for Responsible Use of Digital Connectivity 8

Your role in promoting cybersafety 9

Cybersafety Risk Checklist (CRC) 9

CbD Flow: A Process for Adopting Cybersafety by Design Principles 10

Conclusion: The Evolution of Trust 11

CbD is based on the gold standard in privacy: Privacy by Design.
This paper is freely downloadable from www.PrivacybyDesign.ca.

Introduction

Well into the 21st century, the Internet is no longer an innovative technological utility but a part of our everyday lives. Emerging business models no longer monopolize media attention as much as the frenetic pace of growth of the lucky few that have gained traction against all odds and in some cases, by dubious means of expansion. The drive to perform means that growth is the new metric and users are the new currency.

By raising the profile of rapid growth companies as the ultimate ideal, the media bestows a certain hero status to those whose extreme focus on driving the numbers result in monumental wealth. In so doing, the innovative aspect of the undertaking as well as its real value to the world are lost in translation. In their stead is the artificial, abstract idea - made real by little more than breathless, repetitive coverage in the absence of substance - that if a tribe can balloon to become an army that in turn can anabolically scale to become a *population* in the shortest amount of time, then it has earned its place in the annals of disruptive creations.

In the knowledge economy, ambition is not a flaw. Thinking big offers great advantages but the default framework is currently broken. It allows users to be used, consumers to be consumed and resources to be exploited towards the achievement of a goal that amplifies the risk of corrupt practices, the gestation of malicious intent and the faulty implementation of preventative safeguards to protect individuals. No matter what the quantitative value of risk happens to be, it can always be shifted onto the end user, making the opportunity that much more salient for those positioned to exploit the situation. This applies to online advertising, software publishing and all the models that serve to monetize and derive ROI from Internetworking technologies. The privacy, surveillance and safety risks to users and consumers increase disproportionately with the value they receive from the systems that seek to scale. The relentless growth of big data, aggregated profiling as a result of the mergers of Internet giants, behavioural profiling and targeting technologies are facilitating the introduction of threats that extend beyond privacy into personal safety and real-world, individual assets.

In the summer of 2013, the Information and Privacy Commissioner of Ontario and Claudiu Popa, founder of the KnowledgeFlow Educational Foundation took part in a series of video interviews that laid the foundation for the set of principles now governing Cybersafety by Design (CbD).

Derived from the gold standard in privacy - *Privacy by Design* - a modern blueprint has emerged to provide a framework for a growing universe of social connectivity and the safety measures needed to protect people. CbD is a set of principles that provide leadership and guidance to

- builders of exciting new connective technologies with the potential to make a real impact
- educators whose horizons are constantly expanded by emerging technological innovation
- investors with a keen eye for global demand for positively disruptive change

Ultimately, progress is driven by consumers. The people whose actions steer the future through their adoption of new processes and technologies.

People are the inhabitants of social ecosystems and the stakeholders of the new economy.

Organizations that are able to offer online safety, demonstrate responsibility and build integrity into their operations stand to reap the benefits. Smart companies understand that economic value is not derived from calculations that result in higher physical headcounts or numerically higher 'eyeballs' but in the much more elusive quantity of trust. In other words, if we are the new currency, then our value is the trust we bestow on the systems that facilitate our activities.

Smart change agents know that it's not about how much money one has but about what that money can buy. Similarly, the value of the new currency then is not in its numeric value, but in its ability to derive trust from it. Organizations that exploit the masses without regard for the notion of protective cybersafety rapidly erode human trust and lose economic advantage.

Cybersafety by Design Principles are designed to help protect people and foster trust in systems that empower users and consumers.

The 7 Principles of Cybersafety by Design include guidelines for educators, developers, parents and administrators to employ in the responsible implementation of safe online social networks, learning environments, online communities, Web sites and mobile applications throughout their life cycles. CbD helps to level the playing field between organizations and audiences by asking the tough questions about information use, access, protection and control. Questions of duty of care, disclosure, consent, openness and appropriate use.

What do we mean by *safe*?

The Cybersafety by Design principles hereby define safety as protection from exposure to features and systems that increase the risk of privacy breaches, surveillance, abuse and exploitation of individuals. In-built safeguards that reduce or control the risk are recognized as cybersafety controls and fall into the scope of the 7 Cybersafety by Design Principles.

In building any community program, social application or collaborative information system with touchpoints to personal information, the 7 Principles serve to guide the design, development, deployment, maintenance and promotion of an initiative that meets the criteria for online safety, responsibility and integrity even as the social ecosystem continues to evolve around it.

The authors and the Information and Privacy Commissioner's Office hereby place CbD into the public domain[1] to serve as a framework for responsible design, development, deployment and management of technologies with human touchpoints.

[1] With necessary limitations related to the verifiability of compliance, integrity and rigor of enforcement.

The 7 Principles of Cybersafety by Design

Principle #1: Anticipate and Defuse Online Threats

Being proactive with matters of cybersafety is the only effective approach to addressing threats posed by malicious online activity. The initial step in addressing threats is to identify scenarios, extract individual threats, rate outcomes and document solutions that can be distilled into specific safeguards to, for example, protect youth from cyberbullies or social network users from privacy threats to personal information.

Because of the nature of information, once compromised it is very difficult to control. Reacting to events that have already occurred is a compensating control that, by its nature implies at least some damage has been suffered. To avoid escalation into damage control situations, design teams, project managers and their organizations must anticipate - even qualitatively - the cybersafety risk before creating an overlapping inventory of safeguards to address identified threats.

Principle #2: Cybersafety by Default

Building safeguards into innovative technology solutions, educational programs and social networking must not be seen as a distinctly different development life cycle process. Intrinsically designing cybersafety into all initiatives is the best way to foster trust and encourage full use of the resources made available by today's innovative solutions. When users can assume their safety is protected, that degree of assurance is the very mechanism that unlocks the promise of today's networked, social ecosystems.

Built-in cybersafety can deliver the trust and confidence to strengthen brands and create the good will to enable viral promotion of any valuable initiative. Enthusiastic users will always want to share ways that can benefit their social network. Default cybersafety doesn't just ensure safety, it makes everyone look good ... and for good reason.

Principle #3: Integrity Embedded into Design

Users, learners and participants look at those who create new things as innovators and leaders. They want and need to trust those in charge before any value can be delivered. By placing clear integrity markers within the overall solution, those leaders have an exceptional opportunity to foster the user confidence so critical to the adoption of their initiatives.

By openly disclosing key information and sharing important details with audiences, successful innovators gain the trust to become leaders. It starts by avoiding surprises and continues throughout the user relationship. When those relationships are with young people, the risk and opportunity are both amplified by virtue of the very notion that defines this demographic: comfort. In the absence of palpable integrity, nothing spreads faster than mistrust, but in the presence of trustworthy, established assurance the message - as demonstrated by numerous mobile apps and modern initiatives - will spread like wildfire. Trust is about integrity.

Principle #4: Optimized Experiences with Functional Cybersafety

Fostering online experiences that infuse digital relationships with confidence and trust begins with the end goal. A world where the equivalent of metal detectors and police presence in primary schools is not a positive sum solution to the safety issues of the day. To create a win-win scenario, thinking big, implementing comprehensive solutions with reasonable compromises is a start.

Functionally effective safeguards are unobtrusively designed to provide the comfort to take in value offered by legitimate programs, systems and networks. Accommodating user interest means delivering experiences that are not limited by the natural need for safety and security, nor curtailed by the human right to privacy. Reducing the richness of feature sets compromises user experiences and ultimately limits the potential to effectively reach greater communities and touch more individuals.

Principle #5: Clarity & Simplicity in Execution

Complexity is the enemy of usability. The online world's dependence on a reactive model where transparency reports, terms of service, privacy and security policies have become the norm, the clear goal needs to remain the provisioning of effective solutions that mitigate the risk of abuse.

Cybersafety by design begins with a simple message clearly articulated and easily accessible throughout the entire user experience. User awareness and safety assurance are the building blocks of the most comprehensive solutions. The scalability of approaches for safe use of technology in family settings, for complete user-centricity in systems development and for responsible program development in educational environments is the key to effective end-user protection. Organizations, associations and even families that adopt CbD best practices can therefore ensure the consistent, end-to-end application of simple but overlapping safety measures that effectively represent the foundation of tomorrow's social and digital ecosystems.

Principle #6: Vigilance & Awareness, NOT Fear, Uncertainty & Doubt

By design, CbD embraces an overlapping mesh of cybersafety measures intended to eliminate opportunities for abuse. As a layered approach, Cybersafety by Design's permissive model ensures awareness, encourages vigilance and empowers users with the understanding they need to trust a system with their digital lives.

In so doing, Cybersafety by Design introduces the concept of users as stakeholders whose needs for security and safety must be respected above all else, and the demonstrated approach to this protection is the foundation of that trust. Without evidence that stated promises are supported and objectives are met, without the ability for independent verification (verify, then trust), even the most well intentioned initiative will lose the interest, value and trust it was originally created to garner. Flexibility, visibility and transparency are the key tools CbD champions use to combat fear, uncertainty and doubt (FUD).

Principle #7: Protect Free, Responsible Expression

Exceptional systems that embrace the Cybersafety by Design platform are able to leverage stakeholder trust as a quantifiable asset, enabling their initiatives to leverage the Principles as a springboard to achievement. This achievement is the glue in online communities and binds users to implementors, stakeholders to leaders.

By architecting non-invasive programs, systems and applications that encourage the free expression, exploration and responsible use of available resources, thought leaders create vast networks for information exchange, knowledge transfer and personal growth ... on a vast scale. The alternative is a digital society where individuals cap their emotions, restrict their activity and fear bullying, abuse, intrusion and damage to reputation. These once abstract notions are today very real, with damaging consequences that can only be alleviated by the systematic, assiduous application of controls that protect not only the most vulnerable, but every single, valuable member of each user base, every citizen of our online society and every element in our growing ecosystem of interconnected people & devices - the Internet of things.

A Platform for Responsible Use of Digital Connectivity

By proactively implementing Cybersafety by Design at the outset of every initiative, the intended audiences of academic, commercial and individual entities are able to leverage a rich framework of controls with a common goal: ensuring the quality of online experiences by eliminating negative elements from polluting our social networks.

The 7 Foundational Principles of *Cybersafety by Design*

1. **Anticipate** and Defuse Online Threats
2. Cybersafety by **Default**
3. Integrity **Embedded** into Design
4. Optimized Experiences with **Functional** Cybersafety
5. **Clarity** and Simplicity in Execution
6. Vigilance & **Awareness**, not Fear, Uncertainty & Doubt
7. Protect Free, **Responsible** Expression

The broad, systematic application of Cybersafety by Design is facilitated by the tools, techniques and processes outlined in this document. The authors encourage organizations, associations, groups and individuals in all sectors to use the CbD framework in building, unveiling and scaling disruptively ambitious and overwhelmingly beneficial opportunities that contribute to the rising tide of responsible thought leadership and protect all stakeholders.

Your role in promoting cybersafety

Whether you are an educator, a parent, a developer, belong to a parent council or are a member of law enforcement, your use of digital technologies affects those you communicate with. No one knows your role better than you. That's why every CbD principle uniquely impacts you and your social ecosystem.

We want you to adopt the CbD principles and make them available to your audience. Use the diagram below or the sample questions. Create a checklist, an implementation guide or a presentation and share it. Show others in your space how you implement responsible software features that protect online experiences. Teach young people, older adults and everyone in between how to systematically identify and mitigate online risk. Apply these principles and document your approach in a simple, clear and readily usable way.

The CbD Framework scales to support your scope. All you need is passion and interest. You can have a positive impact on your localized group or across vast social ecosystems. How you use CbD is up to you. We are here to support. Write to us with your ideas and initiatives at CbD@KnowledgeFlow.ca or ask the Office of the Information and Privacy Commissioner of Ontario to connect you.

Cybersafety Risk Checklist (CRC)

- ☐ Does the system/website collect, use, or disclose personal information? How sensitive is the personal information it handles?
- ☐ Does the website or software seem to collect more personal information than is absolutely necessary to fulfill its purposes?
- ☐ Are users required to take specific actions to protect their privacy, or is privacy the default setting? Are user privacy preferences configurable?
- ☐ Can you envision how someone might use this app or site to attack or victimize others? Is the system easy or difficult to abuse in this way?
- ☐ Do you see a compromise between functionality & safety, i.e. offering conditional access to desirable features to the detriment of privacy?
- ☐ Can users trust the system to consistently protect data throughout its entire lifecycle (i.e. collection, use, disclosure, retention, and disposal)?
- ☐ Are privacy policies, terms of use and feature descriptions clearly described, covering all the basic facets of user and data protection?
- ☐ Is it clear to users when and how personal information about them is being collected, used and/or disclosed, and how to report abuses?
- ☐ Does the system include features & dependencies that make it less trusted and more prone to abuse? i.e. covert chat, targeted ads, etc.

CbD Flow: A Process for Adopting Cybersafety by Design Principles

Do you see opportunities to improve privacy or cybersafety?

Use the CRC to gauge risk against the CbD Principles

Phase	Detect	Correct	Monitor
Objective	Identify specific instances in which the system contravenes cybersafety principles	Design and develop new controls to comply with privacy and cybersafety principles	Deploy, suggest and/or periodically review effectiveness of cybersafety features/controls
Key Activities	Understand the system's goals and feature set Evaluate existing system safety controls against *CbD* Principles Identify deficiencies (gap analysis) Document scenarios where users or the public can experience adverse situations due to intentional or accidental abuses	Design and/or build safeguards that meet online safety, security & privacy requirements Create a plan to phase out earlier/ existing non-compliant features Document new features, controls, safeguards, processes, policies Create test scenarios for the testing of features and safeguards against cybersafety principles	Revalidate the redesigned target system against *CbD* Principles Monitor the deployment and on-going maintenance of the system, process or application Confirm alignment with original deficiencies Verify adequacy of evidence collection by monitoring or reporting processes
Outcome	Clear report on project risks and remediation objectives	Concise feature analysis demonstrating efficacy of new vs. old system	Acknowledge and raise awareness about system's adherence to cybersafety

Technical diagram designed to provide a simple template for the success of projects seeking to identify threats or remediate cybersafety risk.

Conclusion: The Evolution of Trust

With the coming 'Internet of Things' and an imminent hyperconnected world composed of intelligent appliances, what will become of our notion of trust? Will we ask fewer questions before surrendering personal information or submitting to automatic monitoring, or will we insist on adherence to basic norms of conduct for future technologies? Will our children consider their personal information a valuable asset to be used as currency in exchange for valuable services? Will our social ecosystems provide opportunities for connecting and monitoring everyone, all the time, or will they incorporate the evolution of the basic principles of Cybersafety by Design?

Time will tell, but instead of waiting, we invite you to find ways to adapt and implement Cybersafety by Design to current and emerging issues in your life. From cyberbullying to privacy abuses, all user risks arising from the use of mobile apps, websites or connected systems arise from the basic failure to implement controls and safeguards to ensure. You see opportunities every day. Pick up the tools, apply the Principles, help close the gaps. Build Cybersafety by Design and strengthen the fabric of our digital ecosystems. You can make a difference *today* on the Internet of tomorrow.