Personal Information Agent™

Take Control of Your Information

Your **security**, **privacy** and **liberty** depend on it.

Do you believe humans have a right to **protect** and **control** their personal information wherever it exists?

Kevin O'Neil, CISSP @CYVAResearch

We all have a human digital existence. As such, I believe we have inherent and inalienable rights and responsibilities to protect and control our personal information, our human digital person wherever it exists. The capability to protect and control our human digital existence, our personal information is essential to our security, privacy and liberty.

We also have a shared mutual responsibility and duty to protect one another, to be vigilant and fight for our hard-won inalienable rights and liberties as enumerated in the U.S. Constitution.

Our Escalating Cybersecurity Catastrophe is Entirely Manmade

Presently there is no end in sight to data breaches, cybercrime, and cyber-attacks by our enemies. Whether these adversaries are criminals, cyber terrorists, cyber bullies, or nation state actors, what

is undeniable is that this cybersecurity catastrophe is entirely manmade.

We have long known the necessity of self-protection in a hostile physical world, the right to bear arms, to be secure in our person, home, papers and effects. Cyberspace is no exception. And presently, our information is weak, vulnerable, easy prey. This is by design.

Information can be used for us (good) and against us (evil). It is critical to understand and know as fact, that our present human digital existence, our personal information is largely out of our control. This is by design.

We are purposely denied authoritative direct control over our personal information, and therefore are perilously unable to prevent having our information used against us (evil). This is by design.

We are all subject to always-on surveillance. Companies are tracking our location, recording our behavior in an expanding network of smartphones, imbedded IoT devices everywhere, cars, homes, appliances, TVs, and AI face recognition capable video camera systems. Our environment, public and private, is systematically being infused with spytech.

Super profiles have and continue to be built and shared across a sea of data brokers, our modern day data slave traders, human digital traffickers who profit from our personal information in advertising schemes, making billions in revenue, while negligently exposing us all to a never ending onslaught of cybercrime and cyber terrorism.

Crony Big Tech and corrupt Big Government maintain this status-quo of maximum control by themselves over our personal information. This is by design.

Our military, Special Operations Forces (SOF) warriors, and their families have and continue to be hunted in this interconnected physical to digital terrain, a cybernetic ecosystem built and operated by a myriad of players, some wholly hostile to our security, privacy and liberty.

This constantly changing world called cyberspace is a battle space, a war zone.

***A war over who owns and controls our human digital existence, our personal information has been raging for years*.**

Our warriors, our military are priority targets for our enemies and like us all vulnerable to a plethora of harms.

Presently, citizens and warriors have little if any control over their human digital existence, their digital identity and information assets in cyberspace.

Our Data is Weak, Vulnerable, Easy Prey. This is by Design

Core to the cybersecurity catastrophe we are experiencing are computer language data primitives, be it C, C++, Java or other languages. These primitive data types such as byte, short, int, long, float, double, boolean and char were never designed to be owner-operator controlled, intelligent, self-protecting, self-governing, self-monetizing.

Neither are commonly used file formats such as XML (Extensible Markup Language) and JSON (JavaScript Object Notation) that are used for storing and exchanging data. They cannot protect or govern themselves and even if you encrypt these files there is no owner-operator post-decryption

control.

JSON example: {"name":"John"}

In other words, the data object is the most fundamental flaw in our critical information technology fabric.

As a result, our information is weak, vulnerable, easy prey.

This is a fundamental flaw and continues to put us all at risk.

Big Tech promotes and maintains a weak-primitive, “dumb data” paradigm as it serves their goals of maximum profit and power: control over our human digital existence.

I argue profit and power-driven Big Tech and Big Government do not want humans to be equipped, augmented with the capabilities to protect and control their personal information wherever it exists post-decryption; to have the power to lock-at-will, erase-at-will, change governing security, privacy and liberty policies-at-will, audit-at-will, and according to our terms and conditions monetize, derive value and/or benefit from the trustworthy use of our information assets.

As a result of this willful negligence, corruption, and anti-liberty malice billions of people are being harmed: identity theft, credit card fraud, medical identity theft, stalked, constantly being tracked (geo-location), messages, photos, biometrics being collected, our online and physical presence under constant surveillance, captured and recorded, comprehensive profiles being built with all of us being set-up, prepositioned for at-will persecution, being cancelled, coerced, imprisoned, targeted for elimination at any time.

All of this spytech infused and purposed surveillance infrastructure, our cyberspace, all of this, by design is a mirror image of tyrannical nation states such as the CCP, Russia, North Korea, Iran, other anti-liberty surveillance states and our deep state bent on ideological, political, cultural and economic domination and tyrannical control over humans domestically and internationally.

Businesses have and continue to suffer billions in stolen intellectual property (IP) losses. These harms to people and businesses are the direct consequences of by design weak, vulnerable, easy prey, ***dumb data*** objects that were never designed to be owner-operator controlled wherever they exist, intelligent, self-protecting, self-governing, self-monetizing.

Disruptive Innovation: Self-Determining Digital Persona™

What if data, data objects were re-engineered, a new class of mobile information agents (HW/SW) designed to be always under our authoritative control (post-decryption), intelligent, self-protecting, self-governing, self-monetizing?

CYVA’s patented Self-Determining Digital Persona™ (SDDP™) is such an invention, a disruptive innovation. It is the basis for our Personal Information Agent™ (PIA™). Our augmented human self now has a human digital persona that is designed to be us (HW/SW), follow our explicit rules, enforce our right of informational self-determination, our values and beliefs as augmented cyber human beings.

AI/MI Code Generation, Maintenance, Human Understandable, Verifiable Rules & Logic Quality Advantage

Our Machine Intelligence (MI) code generator writes the logic for the PIA handler, including its rules and code, producing human understandable documentation, and facilitating/steering its maintenance. The rule generator, used all the way down to program logic, points out contradictions in rule and code logic as well as indicating logic areas that need to be added/enhanced, guiding development and maintenance.

There are concerns with Neural Net based AI that is inscrutable to humans in terms of logic, rules and how it makes decisions, performs work or tasks and achieves an objective, our objectives hopefully. Our approach is to employ AI/MI in such a way that delivered and executed code logic is human understandable, verifiable with transparent assurance of how the system made decisions and performed tasks and achieved our objectives as they relate to and fulfil our human-centric, human-valued (sanctity of human life), ethical choices for security, privacy and liberty in a cyber-physical world.

Further reading: "AI will soon become impossible for humans to comprehend – the story of neural networks tells us why"

The Tensions of Algorithmic Thinking, Bristol University Press, by David Beer, Professor of Sociology, University of York

Security Rule #1: Trust No One

Especially do not trust any individual or organization that does not respect our right to protect and directly control our personal information wherever it exits.

Big Tech monopolies and Big Government maintain a weak, vulnerable, easy prey, ***dumb data*** state of being digital. This is central to their power and means to create vast wealth for themselves enabled by their pervasive out-of-control collection and exploitation of our information.

Our personal information, the primitive data objects that make up our human digital person, were never designed to be self-protecting, self-governing, intelligent, under our direct authoritative control wherever they exist, post-decryption.

Why is it that we cannot directly control our personal information: lock-at-will, erase-at-will, change governing security, privacy and liberty policies-at-will, audit-at-will, and according to our terms and conditions monetize and/or benefit from the trustworthy use of our information assets?

Historical Analogy, A Comparison: Our Auto Industry Then, Our Information Technology Industry Now

Unsafe at Any Speed: The Designed-In Dangers of the American Automobile authored by Ralph Nader and published in 1965 documented the designed-in dangers of automobiles. Our U.S. auto manufactures built cars for 85 years without safety belts being standard equipment. Thousands died.

Today: Our Data Has No Safety Belts

This is by design and millions of people and businesses suffer the consequential cybersecurity, cyberterrorism, privacy, and liberty harms every day.

Unsafe at Any Clock Speed: The Designed-In Dangers of Information Technology would be an appropriate title calling out our present by design dangerous technological reality wherein our weak, vulnerable, easy prey ***dumb data*** is being used against us, not for us.

Solution: Let's Re-Engineer Data (HW/SW)

What if data objects (HW/SW) were re-engineered to be under our direct control wherever they exist, intelligent, self-protecting, self-governing, self-monetizing? Now that is disruptive innovation. Imagine people and businesses in control of their information assets wherever they exist and the resultant accountability (audit-at-will, forensic proof-of-authorization) and much needed strategic improvement in merchant-consumer mutual trustworthiness. Responsible, trusted brand-minded merchants want direct and trustworthy relationships with consumers. Consumers never sell their data; they license it and continuously control it.

There is no end in sight to cybercrime, cyber terrorism and the out-of-control capture, exploitation and profiting from our personal information. Big Tech and Big Government (e.g., CCP, Russia, N. Korea, our deep state, …) architects are partners, working together to maintain this weak, primitive, easy to surveil, easy to collect, easy to exploit and control all peoples design for cyberspace.

And millions of people globally are having their data stolen, exploited and used against them every day.

Our tech industry is in part incompetent, some players I believe are willfully and criminally negligent. Why fix this problem when you are making so much money off a weak, vulnerable, easy prey, ***dumb data*** status quo?

There is too much power in the hands of too few technology giants who wield immense coercive control and influence over so much of our information economy and society, domestically and globally.

Small business cybersecurity innovations are being systematically undermined by monopolies and investment groups committed to the anti-liberty surveillance state and human digital trafficking that generates billions in revenue every year.

The internet as we know is rigged-for-slavery, rigged-for-tyranny. This is by design.

Join us and support our Personal Information Agent™ (PIA™) technology and services development.

Learn more about why Security + Privacy = Liberty and why Security - Privacy = - Liberty (anti-liberty surveillance state).

Take a look at our Personal Information Agent and Trust Community (TC) Operator Kit prototypes, our videos, patents, platforms and services descriptions.

Personal Information Security and Exchange Tool: 5,987,440
Personal Information Security and Exchange Tool: 7,289,971
E-Bazaar Featuring Personal Information Security: 8,195,569

Join us and support the Human Digital Liberty Movement. Sign up for notifications and our newsletter.

CYVA Research is a cybersecurity innovation, strategic research and development firm. Our focus is developing disruptive security, privacy and liberty technologies and strategies for our clients. CYVA's internationally patented Self-Determining Digital Persona™ (SDDP™) technology is an owner-operator controlled, intelligent, self-protecting, self-governing, self-monetizing mobile identity agent (HW/SW).

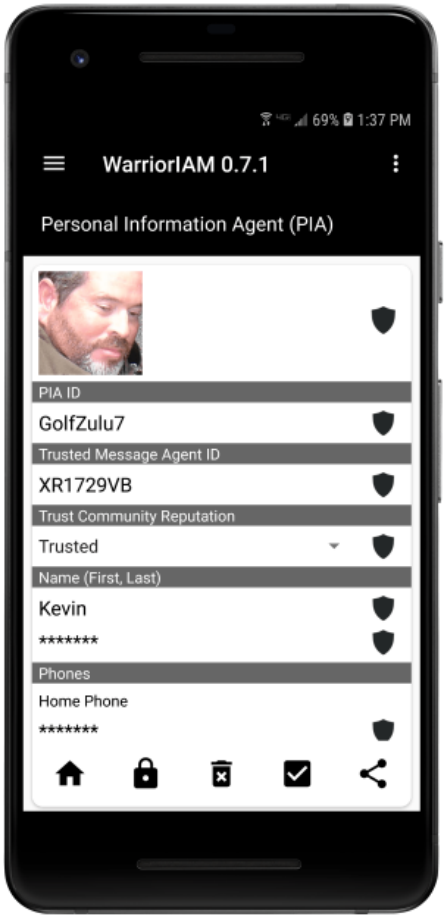
The SDDP™ provides, augments people and communities with the capabilities to protect, control and monetize their identity and information assets wherever they exist post-decryption.

We call this Human Digital Liberty™.

These capabilities are the foundation in forwarding disruptive innovate approaches to the challenges of security, privacy, and liberty in our presently hostile cyberspace.

Our mission is to provide people the capabilities to protect and control their personal information wherever it exists, post-decryption; and according to their terms and conditions derive value (monetize) and/or benefit (discounts) from the trustworthy use of their information assets.

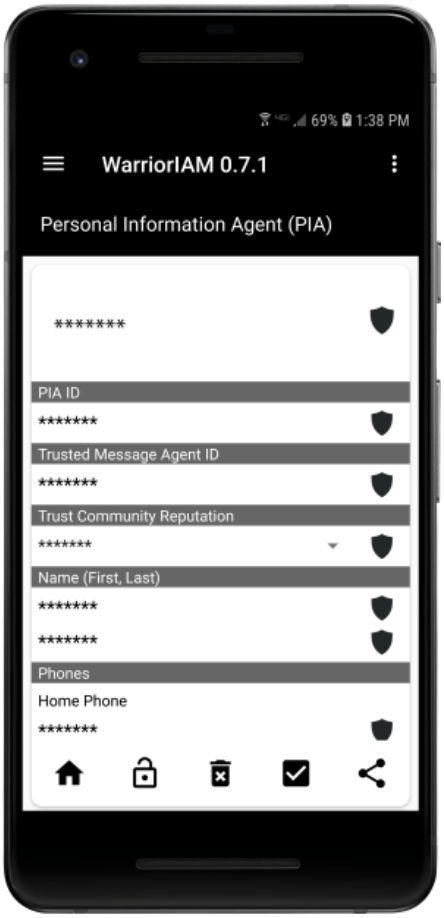
Join the Human Digital Liberty Movement and support our mission.

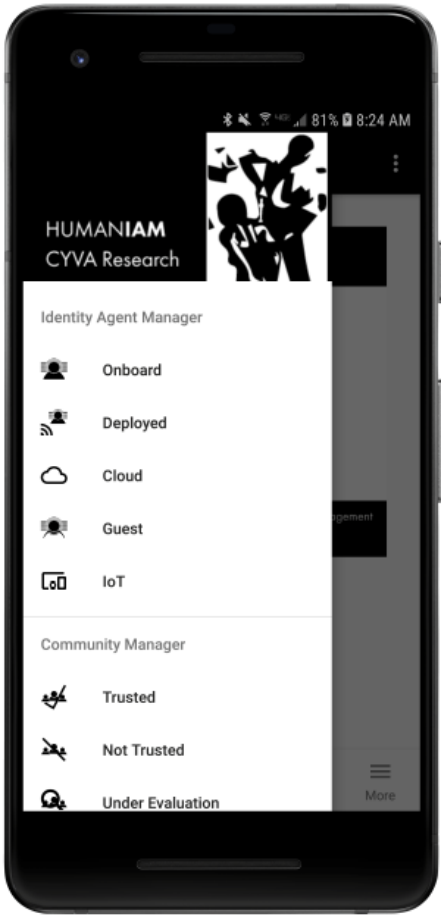


Personal Information Agent™(PIA™)

Provides an individual the capability to protect and control their agent-based digital identity and information assets wherever they exist.

Control Example: Lock/Unlock your PIA™, your PIA-based personal information anytime, anywhere. Enforce your right to authoritatively and directly control your personal information.

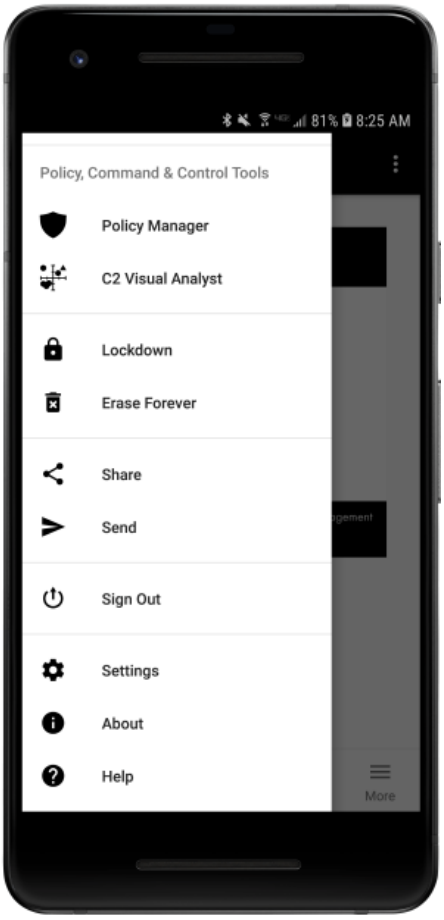


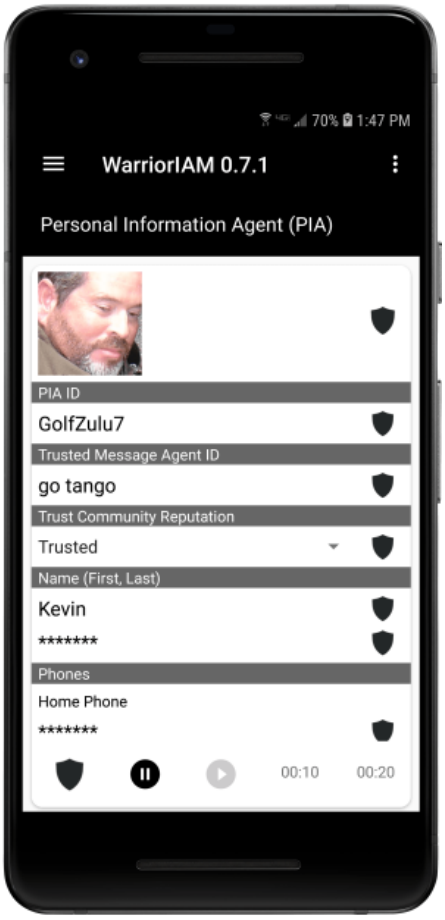


PIA owner-operators author and manage their PIAs with CYVA's

Human-Controlled Identity & Information Asset Management™ (HumanIAM™) platform and services.

Capabilities include providing humans continuous protection and control over their deployed digital identities and information assets wherever they exist across hostile environments; and the formation and management of Trust Communities (TCs).

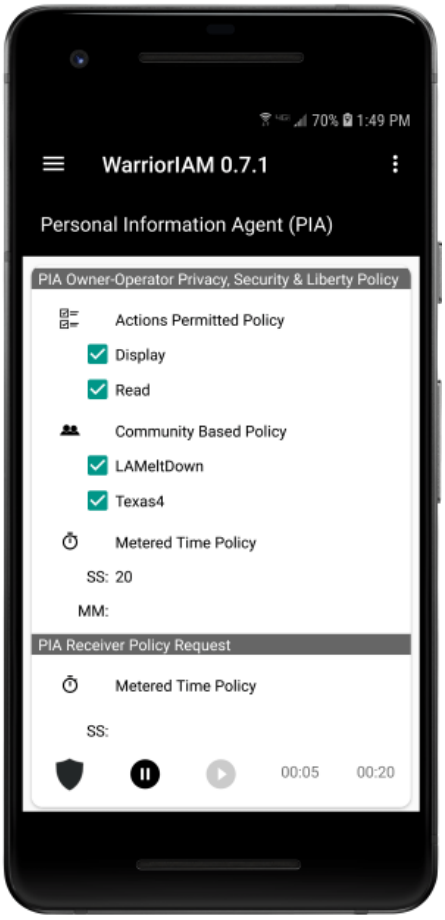




Metered Time Policy

As an example, a PIA owner-operator can set a Metered Time Policy wherein there is a limited amount of time, say 20 seconds that a PIA recipient can display or see the displayed PIA.

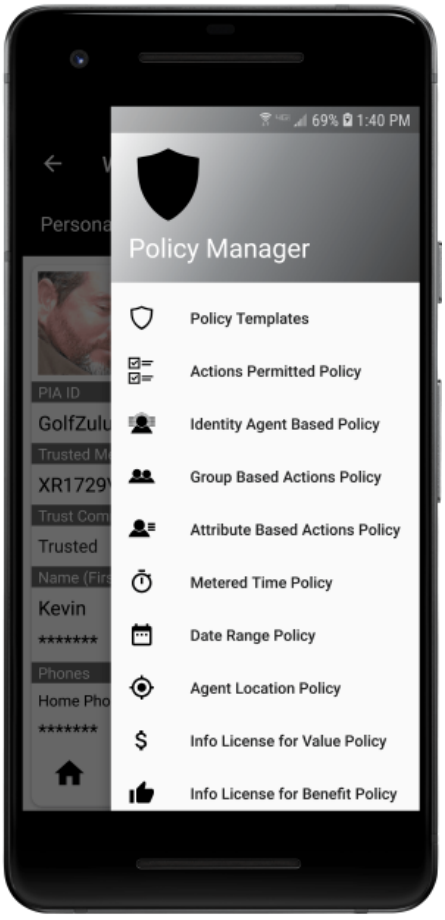
A person might send a picture or a message that is contained within their PIA and limit the display time to 1 minute or 24 hours. The Metered Time policy can be dynamically set by the PIA owner-operator.



PIA Security, Privacy and Liberty Policies

These are your rules, your policies governing your personal information wherever it exists.

Metered Time Policy is one of currently 18 policy types or categories of security, privacy and liberty rules being developed for our PIA Pro version.



These policies are bound/assigned to their identity and information assets and travel with them, always-on, always enforcing their security, privacy and liberty rules.

Human Digital Integrity, Human Digital Dignity, Human Digital Liberty Guiding Architecture Principles

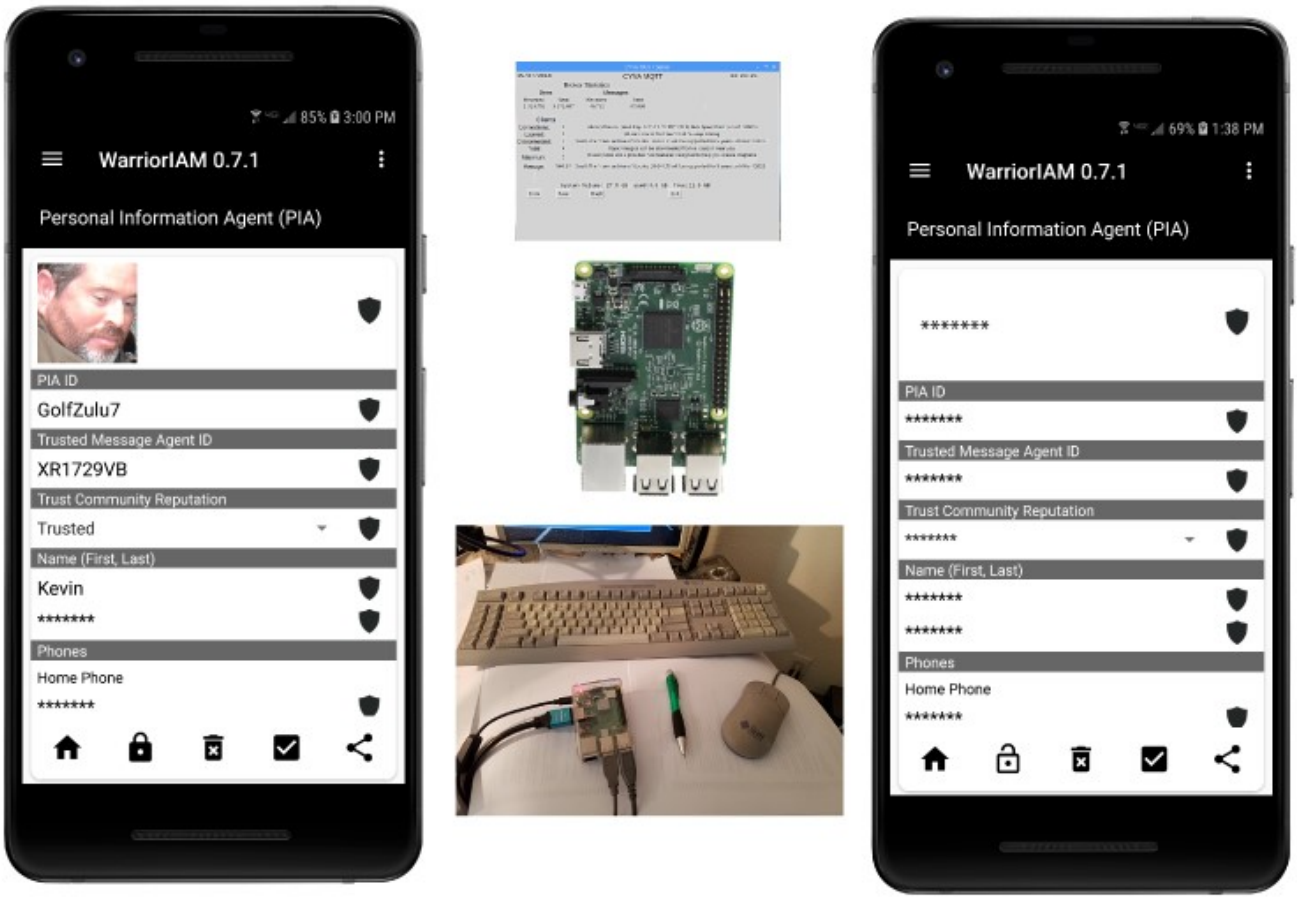
Human Digital Integrity principle: never separate a person's data from their governing security, privacy and liberty policies.

CYVA's Self-Determining Digital Persona™ is built according the firm's guiding architecture principles: Human Digital Dignity™, Human Digital Integrity™, Human Digital Liberty™.

We believe in unalienable human rights and the mutual responsibility to respect and protect those rights in both the physical world and digital world: cyberspace.

We are augmenting humans, amplifying their ability to protect and control their information wherever it exists; and enforce their rights and encourage their mutual responsibilities for security, privacy and liberty for all.

Watch our Human Controlled Identity and Information Asset Management™ (HumanIAM™), Warrior-Controlled Identity and Information Asset Management™ (WarriorIAM™), Augmented Cyber Warrior™ and Augmented Cyber Human™ prototype video.



Trust Community (TC) Operator Kit 1.0-2

Pledge $60 or more to our Human Digital Liberty Movement

Provides Trust Community (TC) operators a high survivability, secure, small form factor, portable kit to independently operate and manage their own Trust Community.

CYVA's TC Operator Kit supports reselling Personal Information Agent licenses: 50% revenue share on PIA annual licenses, and management of TC memberships.

PIA Basic 1-year license: $60/year. PIA Pro 1-year license: TBD.

Our Raspberry Pi-based TC Operator Kit software is distributed as portable Docker containers that include the CYVA MQTT Server and PKI certificate management capability. The CYVA MQTT Server supports PIA to PIA communications, messages, PIA deployments and control.

As a part of our Human Digital Liberty survivability and independence architecture we encourage individuals to form their own Trust Communities and not be dependent on CYVA Research for their

PIA communications infrastructure.

Requirements

Hardware

1 Raspberry Pi 4 or newer

2 Samsung Galaxy Smartphones with Android version 13 or higher

Samsung Smartphone Software

Samsung Knox Platform for Enterprise (KPE)

Optional

Samsung Knox Manage

Knox Manage - Subscription license (1 year) - Win, Android, iOS

MFR#: MI-OSKM110WWT2

Recommended if you want enterprise mobility management made easy with a cloud-based EMM solution.

CYVA Research is a Samsung authorized reseller for Samsung smartphones, tablets and Samsung Knox software.

Includes

TC Operator Kit

2 Personal Information Agent (PIA) Basic Service 1-Year Licenses

We recommend TC Operators have a partner, a buddy-friend TC Operator, a back-up who can manage the TC Operator Kit, co-manage the TC community and demonstrate the PIA technology and services to potential customers.

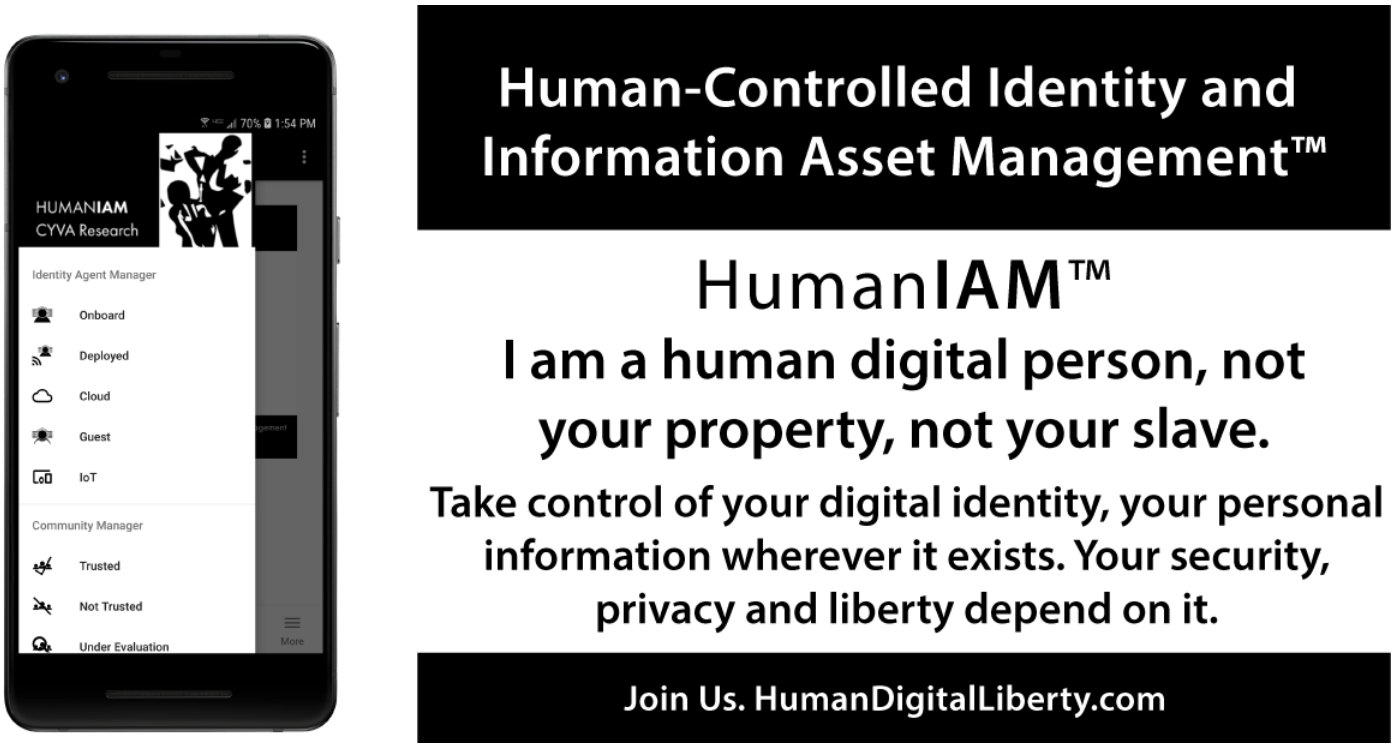
We recommend performing PIA demonstrations as a 2-person team using your own smartphones to demonstrate the PIA-to-PIA remote control capabilities.

You certainly can demonstrate the PIA functionality as a single person. You just need to own two smartphones equipped with the necessary HumanIAM™ or WarriorIAM™ smartphone applications and your own TC Operator Kit.

I often hand one smartphone to a potential customer so they can see the PIA to PIA messaging, lock/unlock, and erase features up close. Watch our prototype video.

Estimated Delivery

The following Human Digital Liberty Movement poster graphics are designed to educate and be shared with others who have an interest in security, privacy and liberty and wish to know more about how to protect and control their personal information wherever it exists.



[Join and support the Human Digital Liberty Movement](#).

Human Digital Liberty™

Take Control of Your Personal Information

Abolish the Data Slave Trade
Human Digital Trafficking
and the
Anti-Liberty Surveillance State

HumanDigitalLiberty.com

William Wilberforce (1798–1879) was an abolitionist, a member of the British Parliament, a leader of the movement to abolish the slave trade, and the systematic dehumanization and exploitation of black men, women and children, Africans during the Transatlantic Slave Trade, 16th to the 19th centuries; The Black Holocaust.

Today we need people like Wilberforce who are motivated to end our present-day Data Slave Trade, Human Digital Trafficking.

This is an industry that captures us, chains us, brands us, declares us all sub-human; declares we have no right to liberty, no right to freedom, no right to informational self-determination. We are declared their human digital property.

This is an industry that generates billions from the exploitation of our human digital person in their data mining, advertising and *surveillance capitalists'* schemes.

Yes, we all have a human digital existence and it is critical we end Human Digital Trafficking, the anti-liberty surveillance state, this rigged-for-slavery, rigged-for-tyranny internet as designed and operated by Big Tech and others.

Recommended reading:

Amazing Grace: William Wilberforce and the Heroic Campaign to End Slavery by Eric Metaxas, November 13, 2007

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff, Mar 3, 2020

Zucked: Waking Up to the Facebook Catastrophe by Roger McNamee, Feb 5, 2019

Dietrich Bonhoeffer (1906 – 1945), was a Protestant theologian, a pastor who openly and secretly from the inside opposed Adolf Hitler and the Third Reich during World War II. Bonhoeffer covertly helped German Jews escape to Switzerland. Bonhoeffer was accused of association with the conspirators of the 20 July Plot on Hitler's life in 1944. He was executed on 9 April 1945.

He did what he could to save lives, oppose the evil of his day and was martyred. He enjoyed a clarity of mind, heart and purpose in his struggle to look deeply into the ethics and duties of a man engaged in spiritual and earthly world warfare.

I hope today's generation will look back at this history, examine Bonhoeffer's life of sacrifice and count the cost, knowing the reality of a Holy Spirit sourced power, peace and joy in dedicating his life to love, honor, and obey God, sacrificially serve people and justly and responsibly oppose evil.

Recommended reading:

Bonhoeffer: Pastor, Martyr, Prophet, Spy by Eric Metaxas, August 1, 2011

Join and support the Human Digital Liberty Movement.

CYVA Research Corporation
3525 Del Mar Heights Road, Ste. #327
San Diego, CA 92130 USA
https://cyva.com

https://humandigitalliberty.com