Security by Infobesity: A Rewired Perspective (2025 Edition)

By Bill Gear

Introduction

In 2013, I proposed a bold theory called "Security by Infobesity": the idea that an individual could protect their privacy by flooding the internet with so much data that it would become difficult to isolate any meaningful personal information. A decade later, the digital landscape has evolved dramatically. Artificial intelligence, data analytics, and machine learning now make it possible to sift through massive data sets with precision. Today, it's time to revisit and rewire that theory to see what still holds and what needs to change.

Part 1: Infobesity in the Age of Machine Learning

Back then, I imagined overwhelming the system would create safety in obscurity. Today, AI systems are not overwhelmed by volume. In fact, they thrive on it. Data is no longer just stored — it's analyzed in real time. Behavior patterns, search histories, purchase behaviors, and even keystroke dynamics are used to build highly accurate profiles.

Machine learning doesn't see a mess; it sees an opportunity. Where I once saw data pollution as protective camouflage, modern algorithms see signal in the noise. Ironically, the more data you create — even junk data — the more data points are available to train AI to understand you.

Part 2: The Evolution of Digital Security Tactics

We've shifted from secrecy and misdirection to a strategy of **minimalism** and **control**. Today's best practice is "data minimization" — collecting, storing, and sharing as little personal information as possible. Encryption, multi-factor authentication, decentralized identities, and zero-trust architectures now dominate secure systems.

Governments have caught on too. Laws like the EU's **GDPR**, California's **CCPA**, and Illinois' **BIPA** put legal pressure on companies to respect personal data rights. Where once the strategy was to confuse the system, today it's to control your exposure.

Part 3: Weapons of Mass Distraction – Still Real

The idea that flooding information systems with garbage would dilute valuable insights still plays a role — but now mostly in disinformation and psychological warfare. Deepfakes, fake news, and coordinated misinformation campaigns exploit the same principle: overload the system until no one knows what's real.

For average users, though, this strategy is more harmful than helpful. Fake personas and misleading behavior can raise red flags in fraud detection algorithms and may even make you more visible to threat actors.

Part 4: Tools of the New Digital Self-Defense

So what's the modern toolkit for digital privacy and security?

- **Privacy-focused browsers** (Brave, Tor)
- **Search engines that don't track you** (DuckDuckGo, Startpage)
- **Disposable email aliases** (SimpleLogin, AnonAddy)
- **End-to-end encryption** (Signal, ProtonMail)
- **Decentralized ID solutions** (like DID or verifiable credentials)
- **Browser fingerprint blockers** (uBlock Origin, Privacy Badger)

In short, today's defense is not to obscure your identity with noise — it's to reduce your trace entirely.

Conclusion: From Infobesity to Informed Minimalism

Looking back, "Security by Infobesity" was a creative approach to a growing problem. But in a world driven by pattern recognition, flooding the system doesn't help you disappear — it helps define you.

Now, the smartest move is **informed minimalism**. Understand what data you're sharing, why, and how to limit it. Use tools that empower you to take back control. The battlefield has changed — and so must our strategy.

Your identity is no longer something to hide in the noise. It's something to secure through awareness.

Interested in the original version from 2013? Check out "Security by Infobesity (Original Essay)" for a look at how far the conversation has come.