# 2 SURVEILLANCE

## ISSUES AND ETHICS

**The Transparent Society:** Surveillance above, sousveillance below. How it came to be. ■ **p. 12**

**Privacy** and **Anonymity:** Not just for people with something to hide. ■ **pp. 26** and **29**

**Power Dynamics:** Transparency does not mean automatic accountability. ■ **pp. 26** and **28**

**Info Control:** Who controls your information? ■ **p. 27**

**Truth:** What happens when reality is faked. ■ **p. 29**

**Insecurity:** How the panopticon increases risk. ■ **p. 30**

**Open Culture:** Transparency breeds tolerance. ■ **p. 31**

## TOOLS AND TRICKS

**Sensor Types:** The many ways we can watch each other. ■ **p. 32**

**Data Correlation:** The amazing things you discover when you analyze massive data sets. ■ **p. 37**

**Countersurveillance:** From privacy mode and blind spots to jamming signals and deceiving watchers. ■ **pp. 38, 41–44**

**Fake ID:** Many ways to change who you are. ■ **p. 39**

## IDENTIFICATION

**ID Systems:** From brainprints to nanotats. ■ **p. 20**

**Resleeving** and **Travel:** How your ID works in new bodies and places. ■ **p. 21**

**The SAPIENT Initiative:** Does it protect your identity or make you easier to spy on? ■ **p. 23**

**Identity Theft:** How your ID can be stolen—and what you can do about it. ■ **pp. 24–25**

**ID** and **Forking:** Can the real you please stand up? ■ **p. 25**

**Source:** *When the Emperor Wore Clothes,* by John Perry Schneier [Link]

Lifeloggers capture every instant of their existence for their own reference. XP stars live, love, and die with passionate abandon so everyone can enjoy it on demand. Habitats depend on constantly updated operational and environmental data as well as troops of transhuman observers to function seamlessly and provide the day-to-day necessities of transhuman life. Hypercorps, governments, organizations, and individuals safeguard the information they need to survive and seek out what they need to thrive. People can access the locations and live streams of their children, friends, loved ones, or complete strangers at whim. Muses regularly access the social profiles and public records of everyone their patrons interact with, transforming total strangers into familiar faces, before greetings are even exchanged. Knowing what's going on across multiple fronts simultaneously is absolutely vital to survival after the Fall, and the only way to do that is to employ a panoply of technologies and behaviors designed to keep track of everything. Technology has enabled universal perfect recall for everyone and for most of the devices they use on a daily basis.

Who watches the watchmen?

Everybody. Always.

## OUR TRANSPARENT SOCIETY

"I'll admit I'm underhanded. The reason that none of you could find vid of my birth is that there isn't any. This task was meant to show you the limits of data mining when you don't have a complete personal history. The three of you who submitted links to your own fake films will receive extra credit. Jeung, however, you're losing points because you got my natal phenotype wrong despite that being public record."

—Rokuzawa Chi, Prof. of Individuality Studies, Titan Autonomous University

"Shit, she's old."

—Abwe al Sul, Junior in Memetics

As social animals, humanity's voyeuristic tendencies seem ingrained. We monitor our neighbors and peers, staying on top of trends and keeping up with whatever is hip and fashionable. We seek out news, because what impacts others may impact us personally. And we love to keep tabs on the glamorous and powerful, hoping to get a glimpse of their exotic lives or whiffs of their secret plans. Similarly, those with something to protect, whether it be wealth, secrets, power, or loved ones, keep a wary eye on those that may pose a threat. Information is gathered to keep ahead of rivals, to market products more efficiently, and to control the masses more thoroughly.

Counter to these spying instincts is our innate desire for privacy, to keep our personal affairs to ourselves, to have the freedom of anonymity and secrecy when we desire or need it. The intersection of privacy and security has become a contested area in recent centuries, a confusing exchange due to competing and sometimes overlapping interests. The inexorable advance of surveillance technologies and digital networks seemed at first destined to undermine fundamental concepts of privacy and personal freedom, sparking fears of Orwellian police states and information dictatorships—until the democratization of such tools turned the tables. Now, after the shockwaves of such disruptive technologies have passed, transhumanity has largely adapted to an open society, albeit to varying degrees. To understand this current state, we must evaluate the path that brought us here.

### THE ASSAULT ON PRIVACY

The rise of pervasive surveillance occurred contemporaneously with the technological and societal changes of the 20th and 21st centuries. Well before the Fall humans were developing ever more pervasive means of documenting their lives and actions. The growth of computer networks in the late 20th century created new opportunities for collecting, archiving, sharing, and cross-indexing data. Old analog records were digitized, increasing their accessibility, making it easier for governments and corporations to share information and track people. New databases sprung up by the billions, sparked by the ease of collecting and manipulating data online. Early users of the internet were largely ignorant of the trail their activities left online, and the many ways in which companies discreetly gathered information on their habits, interests, and personal details, creating detailed profiles of individual users. While many of these archives were bought and sold in private for marketing and commercial purposes, others were left open for the public, making it easy for millions of amateur sleuths to gather information on others. People increasingly found it difficult to escape their pasts, whether it be marred by bad credit, poor driving records, or criminal violations. Even records that were presumably private and restricted, such as medical histories or financial records, suffered from poor security, becoming the victim of public breaches. Criminal networks arose that were dedicated entirely to trading and selling credit account access or compromised accounts to private archives.

The spread of centralized communications networks also enabled new capabilities for surveillance. Whereas harsher regimes shirked no opportunity for monitoring communications in order to root out dissidents and other challenges to their authority, more democratic regimes were marked by widespread civil liberties that restrained government snooping. Nevertheless, as communications channels became increasingly networked, even these more liberal states found excuses to engage in widespread spying. Financial transactions to other countries were subjected to heavy monitoring to deter money laundering, tax evasion, and similar financial trickery. Spy agencies enacted vast data mining efforts to sift through immense amounts of voice and data communications and "listen" for keywords, forwarding any interceptions that raised flags for closer analysis. Wars against drugs, terrorism, and other causes were used to legitimize initiatives for systematic surveillance and further erode privacy safeguards. Security was increasingly the buzzword argument applied to justify border checks, tap communications, access private records, and institute mandatory identification cards and similar measures. Many governments grew so voracious for information that intelligence gathering became SOP for everything from civic programs to embassy relations.

## RESISTANCE TO BIG BROTHER

Privacy advocates were not without support or resources and were largely rooted in hacker and cypherpunk subcultures. In addition to lobbying for privacy rights and creating awareness of creeping surveillance conditions, they established the first digital tools for anonymization and encryption, enabling people to interact online without fear of tracking. These tools were embraced by dissidents, whistleblowers, criminals, people living under oppressive regimes, and anyone else desiring to keep their activities secret. Their adoption was limited, however, as their use (or even awareness of their existence) often depended upon a non-amateur level of technical proficiency. They were also engaged in a constant arms race against new surveillance measures and repressive governments and businesses who would shut their distribution sites down or criminalize them.

## LIKE THIS

A major turning point in the war on privacy was the widespread embrace of online social networks. With the increasing capability to share the minutiae of their lives instantly via the web, humanity stumbled into a participatory panopticon. Status updates, microblog postings, photo and video feeds, and other publicly accessible media streams created a self-maintained, searchable, and public record of most people's lives. Many people integrated themselves into the public domain without any thought to the implications of their participation. By opting in, it was easier to keep up with more friends in greater detail, maximize social and professional exposure with less time, and partake in slices of thought, public discourse, and new participatory media. Opting out reduced an individual's sphere of influence and notoriety and risked branding oneself as a technophobe.

The companies that sponsored these social networks were financially motivated to increase the amount of data people shared online, so early models were designed with minimal privacy options or with such features turned off by default. Participants were increasingly steered towards making their profile, data, and activities public. As a result, those who wished to participate but maintain some privacy were forced to develop information management skills, as they attempted to control how their data was shared and with whom. New generations grew up in this networked world, never aware of life before social networking, thus embracing a drastically different and more nuanced concept of personal privacy than previous generations.

Considerations of who really owned the data posted on these networks and rules governing its fair use and reproduction rights were ignored by the majority. Even when serious concerns managed to rise to the level of public awareness, the benefits of continued participation usually outweighed the psycho-sociological value of personal privacy. By the mid-21st century, most of the world was well aware that they were active participants in a global information system that recorded most of their lives. Privacy was something controlled with check boxes in profile settings, and data was meant to be shared.

## REPUTATION GROWTH

The formal reputation networks that exist AF arose organically from the informal social media developed through the 21st century. An early barrier to interacting with strangers online—particularly when engaging in financial transactions—was not knowing if the person you were dealing with was reliable. Primitive reputation scores were the first solution, enabling buyers to rate sellers. These systems rapidly spread to social networks, discussion forums, and filesharing sites, as a way of valuating participants. Concurrently, for the first time, individuals had access to the same public presence capabilities and image-making techniques formerly reserved for those retaining expensive PR firms. Individuals with huge friends lists and blog followings had commercial pull that could sell products, fill clubs, top up campaign coffers, propagate memes, and make or kill trends.

Likewise, companies and social organizations seized an opportunity to more carefully control their public image for increasingly savvy consumers, in an attempt to manage the ratings their products and services received online. Corporations created