INFOSEC
INSTITUTE

Human Beings, Privacy & the Future of It All

By Susan Morrow

infosecinstitute.com

Executive Summary

Privacy can mean many things, but in general terms, it is about control and consent. Let's take an example: your friend suddenly reveals on Facebook that you are moving home. This action might leave you feeling aggrieved, as it was done outside of your control and without your consent. You may not actually mind this fact being shared with others, but you may mind that you were not consulted. Privacy belongs to the individual and should always be under that individual's control.

Privacy often sounds like an abstract concept. It also gets mixed up with data security; although the two are intrinsically linked, data security can ultimately help to enhance some aspects of privacy. Privacy is also an intrinsic part of our humanity. It works within our relationships with others — if you respect my privacy, I will respect yours.

This is also true in the digital world. The way we interact with technology reflects how we interact with the non-digital world. This is becoming truer as technology interacts more closely with us, using our personal data to do digital jobs. Privacy is not something that technology should take from us, but instead be designed to work with us.

This paper will look at the human side of privacy and how privacy is an intimate part of our relationship with technology. We will look back to look forward to show that while technology can and must use our personal data to create better ways of living and working, it also must do so with privacy as a fundamental part of system design.

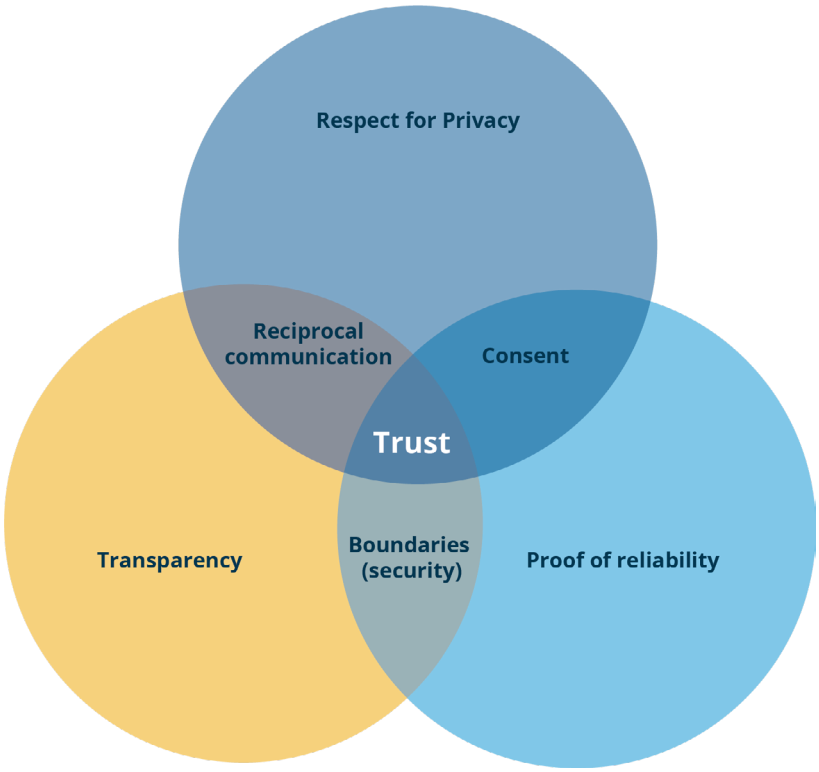
Table of Contents

Part 1: Digital Relationships, Trust & Privacy

If you stop and think about what it means to be human, what do you think of? Being alive means having relationships. Relationships are based on trust, built up over time. And, for a software/system designer, trust is demonstrable. If we tell a secret to a friend and they tell another person without our consent, and then we find out, our trust in them is impacted. Privacy is then a factor within a "Venn of Trust" and is a crucial part of our relationships with others and with technology.

The Venn of Trust

Trust is made up of a Venn of other things and includes respect for the privacy of other people. This is true for all relationships, including digital ones.



Technology, Privacy & an Extension of Us

Privacy is an intrinsic part of human ecology. We build our cities with privacy in mind. Good workplaces are designed to improve productivity by providing private work areas. Privacy gives us a feeling of control over various aspects of our lives and our relationships.

This feeling of control extends to the digital realm. Technology has shown itself to be not just a tool in the workplace, but a complement to our everyday relationships with others.

Social media has demonstrated this perfectly because we are social animals. In 2018, there were almost 3.2 billion individuals using social media of some form – i.e., almost

Any technological system that requires a human being to interact with it and perform, for example, a transaction, needs to be built on trust.

half of the world's population. Considering that digital social media has only been around for 20 years at most, this is a rapid expansion of a specific technology type.

There are currently 5.13 billion users on mobile phones, and 4.02 billion humans are navigating the Internet. Like our non-technological habitat, our technological habitat is built on relationships. These relationships translate to a myriad of transactions — banking, buying, chatting, dating and so on. To keep these relationships working, they have to be built on a backbone of trust. In technology terms, this is achieved by applying security measures to the transactions.

But it also needs to be privacy-respectful. Privacy, as we mentioned earlier, is a deep-rooted part of the Venn of Trust and without it, trust breaks down.

Trust, Relationships & Privacy

Any technological system that requires a human being to interact with it and perform, for example, a transaction, needs to be built on trust.

Identity management is a case in point. Identity systems are a way to control access to resources and to prove something (e.g., you really are you) to allow a transaction to proceed. Identity systems need to be built with trust as a design remit. Privacy, as part of the Venn of Trust, proves your system is trustworthy and helps to build relationships.

Part 2: The Here & Now of Privacy

Privacy is part of trustworthiness which is part of our habitat — both natural and digital. But privacy has not been intrinsic in the design of our technology platforms. Let's take a look at the privacy landscape over the last few years.

The technology community has been aware of data privacy for a while now. The International Association of Privacy Professionals (IAPP) was founded in 2000 as a professional body to look at best practices for data privacy. Organizations like the Electronic Privacy Information Center (EPIC), founded in 1994, are activists for privacy. But the idea that privacy is an important aspect of our technological lives has been around in regulatory frameworks for decades. The European Union's Data Protection Directive (DPD) and other data protection laws such as the UK's Data Protection Act (DPA), which go back to 1995 and 1998 respectively, had at least the mutterings of data privacy with principles such as:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." (UK DPA, 1998)

But as far as data privacy catching the attention of the general public, it wasn't until the

Snowden revelations on U.S. surveillance of citizens back in 2013 that the importance of privacy hit home. The Snowden leaks acted as a catalyst in raising awareness across the public arena.

Here we will look at a few of the most notable privacy events in recent years:

Privacy Debacle Timeline

June 2013 — The Snowden Affair
Edward Snowden, a contractor for Booz Allen Hamilton, stole top-secret files from the National Security Agency (NSA). The files revealed a series of privacy misdemeanors, including a program called Prism, which collected the personal data of the users of services such as Google and Facebook.

Ongoing — Facebook
The company has had privacy issues since its inception. The privacy settings in a user's Facebook account were described by many in the industry as getting worse over time, not better. In 2009, EPIC filed a complaint with the FTC about Facebook's misuse of users' personal data; Facebook settled this claim, agreeing to tighten up consent rules in 2012.

Privacy is not just about data protection, it is also about the use of your data.

One article from 2010 by the Electronic Frontier Foundation (EFF), details the general erosion of privacy by Facebook over time.

However, it was the Cambridge Analytica debacle of 2018 that really saw the gloves come off. Facebook allowed political influencer and data analyst Cambridge Analytica to use the data of 87 million users without consent. Facebook's privacy issues continue, and some would argue, may well be the platform's downfall.

Ongoing — Sidewalk Labs & Sister Company, Google
The name of Google is almost synonymous with lack of respect for data privacy. In 2012, Google agreed to a $22.5 million settlement with the FTC over misrepresenting its use of Apple Safari to users — stating that it would not use tracking cookies to serve up targeted ads, when in fact that's exactly what the company did. Most recently, Ontario's former privacy commissioner, Ann Cavoukian, resigned from a role as an advisor to Sidewalk Labs (a sister company of Google) because of privacy concerns with a smart city project they were working on in Toronto.

Here & Now — Amazon
Amazon is a behemoth that touches many aspects of our lives. The onetime simple bookseller now has smart devices like the Amazon Echo (Alexa) that interact with us on a daily basis. And Amazon holds a great deal of data about us: our accounts have personal data, including financial data. They also have purchase data which can give enormous insight into our lives. With the advent of the digital assistant, Amazon also has more intimate details.

Privacy is not just about data protection, it is also about the use of your data. Alexa has already exposed the data of at least two individuals — in one case, 1,700 voice recordings of one user were given to another user who asked for access to their data under the GDPR.

Note that the list above is far from exhaustive. These are just the cases that made big headlines and brought the issue of data privacy to the front of people's minds.

Good Fences Make Good Neighbors

This build-up of privacy mishaps over the last 10 years or so has now become entrenched in the consumer psyche. Privacy, once an academic discussion only entertained at privacy conferences by lawyers, is now a topic of conversation over the dinner table. The privacy spillages of the big tech corporates have made us all feel vulnerable.

Companies have paid for their disrespect for our personal data privacy. Facebook had $119 billion wiped from their value after the Cambridge Analytica scandal. A Google+ flaw which impacted user data saw a 2.3% drop in share price for the company.

Like the Robert Frost poem which states that "good fences, make good neighbors," good data privacy creates good relationships.

Consumer expectations for privacy and, in turn, trust are at an all-time high. A TRUSTe survey found that 89% of Internet users are "worried" about data privacy. Backing this up is research by Kristin Martin of George Washington University, who found that when privacy is violated, customers' trust in a website will diminish.

Where does this leave us?

The concept of Privacy by Design (PbD) was first developed by Ann Cavoukian. In her treatise on the idea, she set out seven foundational principles which created a framework for ensuring data privacy for the individual. These principles need to be followed by technology designers when creating tools and solutions and during the implementation of technology. When privacy is a design remit, it becomes intrinsic to our use of technology.

Like the Robert Frost poem which states that "good fences, make good neighbors," good data privacy creates good relationships.

Part 3: Privacy, Smart Cities & the Future of Humankind

As technology becomes ubiquitous in everyday life, as the Internet of Things (IoT) makes our homes, our offices and our cities smart, data privacy needs to go along for the ride. We are rapidly moving towards a time where data, including personal and sensitive data, drives our everyday living. The data needed to oil the smart city will be generated by sensors that are in our homes, our cars, on our streets and in our places of work. A number of smart initiatives across the globe are starting this move toward smart living. Some examples include:

Toronto, Canada

The city is known for its heavy traffic and has begun a smart city living initiative called "Quayside." The project is looking at using technology to improve neighborhoods and enhance sustainability. The initiative is looking at smart transport, innovations in energy and waste. The website about the project states that they are doing this "without giving up the privacy and security that everyone deserves."

Toronto partnered with Sidewalk Labs which is owned by Alphabet Inc. (who also own Google). As mentioned previously, privacy commissioner Ann Cavoukian recently resigned as advisor to Sidewalk Labs when they announced that they could not guarantee that the data collected would be de-identified at the source.

Barcelona, Spain

This smart city initiative applies the "Data Directive" to govern the use of personal data. The directive sets out the levels of data sovereignty, privacy and security to be applied during the design of any smart city infrastructure.

No matter what technological process is used, no matter where data goes, how it is collected, used and reused, the person that it relates to must be in control of its use.

The city is mandating the use of the DEcentralised Citizens Owned Data Ecosystem (DECODE). This looks at using citizen data for the wider benefits of the city populace but with privacy as a design remit. DECODE is an EU-funded consortium which is exploring ways that open data can be used in smart cities, like Barcelona. The remit for their connected service in Barcelona is to offer control to the owners of data.

What is interesting about these and many other smart city initiatives is that data privacy is being identified as an integral part of the technology used in the city. However, as the Toronto example shows, there may be more lip service than a commitment to PbD.

Layers of different types of technology are now adding complexity too. Methodologies such as machine learning are being applied to big data analytics. This will bring greater challenges in the control of data.

Can Compliance Help Protect Data Privacy in a Complex Digital World?

Regulations, such as the earlier-mentioned UK's DPA and the EU's DPD, have recently been updated in an attempt to bring them in line with modern hyper-connected data processing technology and the Internet. The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act are modern data protection laws which attempt to address the privacy needs of the modern human habitat. Accountability is an overriding requirement of the modern data protection regulation. The laws stipulate that data processing across the entire life cycle is done with the consent and knowledge of the user — data subject rights being explicitly upheld throughout that life cycle.

No matter what technological process is used, no matter where data goes, how it is collected, used and reused, the person that it relates to must be in control of its use. The only way to achieve this level of control is to have privacy-related functions and features baked into the very fabric of a system.

Privacy is never an on/off switch. It is about nuanced personal choice and control.

Privacy has an intimate relationship with the data, the person it represents, the service that uses it and the technology that facilitates its use. When we build our systems, we need to be highly cognizant of these relationships.

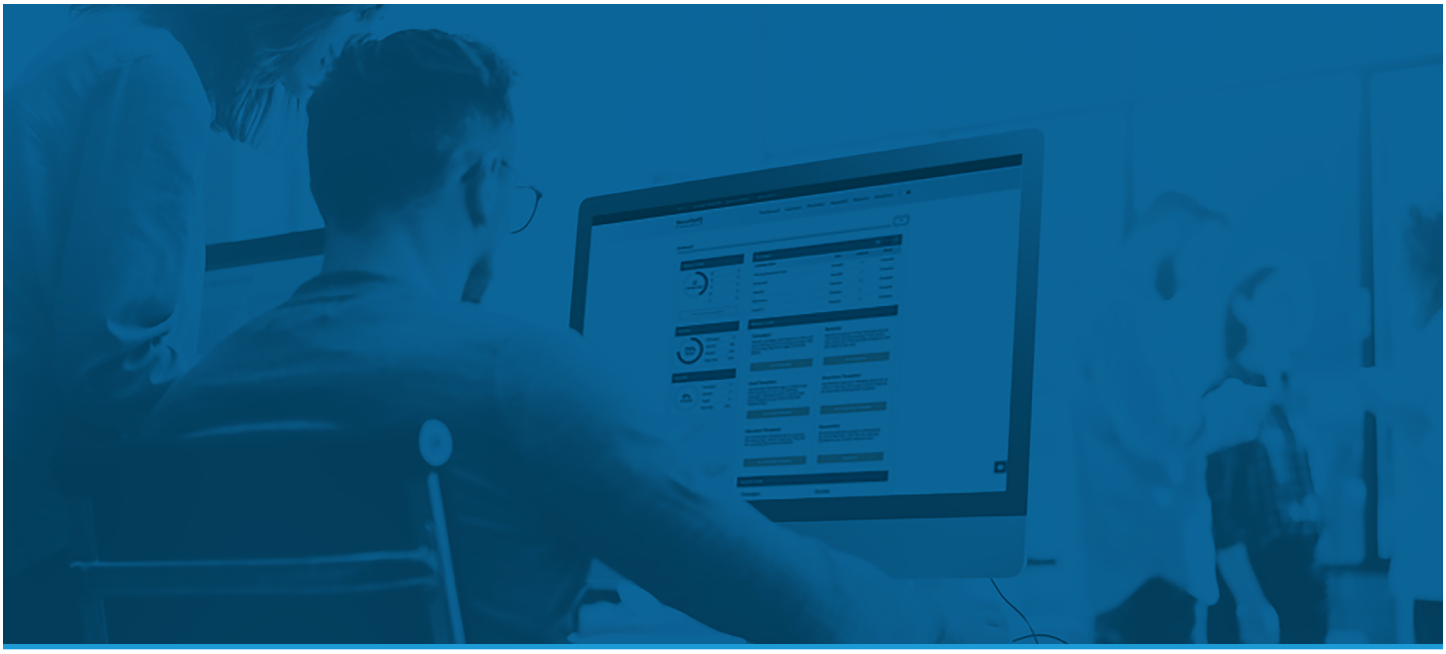
Conclusion

The interaction and connections between us, technology and our data are fuzzy and interwoven. It is a real challenge to build systems that are cost-effective, have great usability, function well and preserve privacy.

Technology can and must use our personal data to create better ways of living and working. But it must do so with privacy as a fundamental part of system design.

The decisions about the design of our digital habitat cannot be left to one discipline. The software upon which we base our digital lives, and which now is intertwined with our non-digital habitats like our cities, must be created by multidisciplinary groups. These groups must include people who understand people.

Privacy is an important aspect of human behavioral ecology. It is the cement of trust, without which trust crumbles and falls apart and, in turn, our relationships suffer. The tech giants who flout our privacy are starting to feel the impact of this. Technology can and must use our personal data to create better ways of living and working. But it must do so with privacy as a fundamental part of system design.



About InfoSec Institute

InfoSec Institute fortifies organizations of all sizes against security threats with award-winning information security education. Recognizing cybersecurity is everyone's job, we provide skills development and certification training for IT and security professionals while building your entire workforce's security aptitude through awareness training and phishing simulations. Recognized as a Gartner Peer Insights Customers' Choice for Security Awareness Computer-Based Training, InfoSec Institute is also a Training Industry "Top 20 IT Training Company" and the Security Training & Education Program Gold Winner in Info Security Products Guide's Global Excellence Awards.

---

infosecinstitute.com

INFOSEC
INSTITUTE

Sources

1. The Rise and Fall of a Neolithic Town, The Çatalhöyük Research Project
2. Global Digital Report 2018, We Are Social
3. How did Homo sapiens evolve?, Science Magazine
4. Building relationships using digital identity, CSO Online
5. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, EUR-Lex
6. Data Protection Act 1998, legislation.gov.uk
7. Facebook's Eroding Privacy Policy: A Timeline, Electronic Frontier Foundation
8. In the Matter of Facebook, Inc., EPIC
9. 'Not good enough': Toronto privacy expert resigns from Sidewalk Labs over data concerns, CBC News
10. Amazon sent 1,700 Alexa voice recordings to the wrong user following data request, The Verge
11. 89% of British internet users are worried about online privacy: report, TRUSTe
12. Privacy by Design: The 7 Foundational Principles, Ann Cavoukian
13. Ann Cavoukian, former Ontario privacy commissioner, resigns from Sidewalk Labs, Global News
14. Bogucki, B., "The Origins of Human Society," 1999, Blackwell Publishers
15. Carter, G., & Wilkinson, G. (2013). "Does food sharing in vampire bats demonstrate reciprocity?" Communicative & Integrative Biology, 6(6), e25783
16. Kirsten Martin, "The penalty for privacy violations: How privacy violations impact trust online," Journal of Business Research, Volume 82, 2018, Pages 103-116