

PETER HESSELD AHL
GROUND RULES FOR THE 21ST. CENTURY
Chapter 19

GOODBYE ANONYMITY

Privacy and anonymity are amazingly sensitive topics. We consider it sacred, as a fundamental right, that we are allowed to be left in peace and that we can decide for ourselves what others should know about us. We need a space where we are totally private and we need sanctuaries where we cannot be assessed and kept under observation.

It is as if we bear a traumatic memory of the small village back in history where people lived so close together that everyone knew almost everything about each other. Compared to the freedom we have today, the social set-up of the past seems suffocating. You couldn't just move, you couldn't divorce, you couldn't close the door to your own room, and you generally couldn't stray very far before you were firmly put back in place.

Being ir-responsible and un-committed is part of the heady feeling of jumping into life in a big city. There is a certain anonymity; you can jump from one thing to another, you can take on different roles, you are not judged beforehand on your entire family history. You can develop, and start over again, if you fail in the first try - or if you get bored and tired and just want to try something else.

The anonymity we have become accustomed to - in cities and in recent years on the Internet - is being reigned in again. The trend is clearly toward more detailed recording, storage, analysis and pooling of information on virtually every aspect of our lives.

It is an extremely sensitive issue - and it is filled with paradoxes. The modern, independent person feels intruded upon if others survey us without explicit permission. Yet the very same person will spend considerable energy on making himself or herself visible on the web.

Technological progress will make consequences visible, so we each understand what our actions entail. At the same time, technology will make it visible to others what we do - and thus we will be much more able to hold each other accountable.

The technologies we used in the past, only to a very limited extent led to the recording of our actions. When we sent a letter in the mail, had a telephone conversation, bought a ticket, borrowed a book or purchased a product, it was normally only something that those who had been directly involved in the transaction, knew about. But for each function where we begin to use digital technology, there will now be an electronic trace: When we send an SMS, when we walk down the street, when we hear a melody, when we use the car's GPS, when we seek information on the net.... If you try to add up, how much information is stored about your actions, it is an amazing number of details - and we are still only in the early development towards registration and transparency.

Anonymity has a price

The registration and sharing of so much data is a prerequisite for the convenience and efficiency, which new technologies can offer us. Yet, at the same time we insist on our right to move about without being traced and without the risk of later being confronted with our actions. We want privacy.

In a historical perspective this is quite reasonable. Times change, and what's normal today, can suddenly turn out to be fatally controversial in a new cultural climate. Groups such as Jews, homosexuals, and socialists have experienced how volatile the norm for what is acceptable can be.

Anonymity is also a safety valve, allowing controversial views to come forth. Unfortunately, the world is dotted with regimes that oppress their people and any attempts at political change. In those situations it is essential that there are opportunities to speak against the dictators and to organize opposition out of sight of the oppressors. Anonymity is the last bastion of free speech. Everything freezes, if you cannot propose change without being persecuted for it.

In some ways, the same mechanisms are at work when it comes to anonymity at the personal and social level of everyday life. Each of us needs some flexibility in how we present ourselves to others.

We have complex personalities, and it's not all the parts of our personality that necessarily match everyone we pass.

We need room to explore and experiment without having to be held accountable to everyone. That space is a crucial part of being a free human.

The difficult question is, how large should that space be?

In Chapter 11, on opening up for what the world can contribute, we discussed how it is a precondition to start cooperating, that the parties trust each other. Confidence comes from knowing that you are able to hold your counterpart accountable. It disciplines the participants when they act in *the shadow of the future*: when each knows that their actions are seen and assessed. Too much anonymity erodes confidence in the system.

Anonymity is essential, but it has a price. It makes it possible to act without consequence. You can free ride and behave in ways that would make the community break down, if everyone did the same.

Assuming responsibility

Freedom is closely linked to responsibility. Each of us has been given more freedom, more opportunities - and therefore greater responsibility - to create our own life. But as we get more responsibility, we will increasingly also be held accountable.

Networking technology gives many more people access to contribute with their different ideas and knowledge. The ever greater connectivity opens up to countless new win-win interactions and relations criss-crossing countries and cultures. But the tight coupling in huge systems also means that we become extremely vulnerable. A single person or a few people can do extreme harm to the entire system - and unfortunately, it is not just a theoretical possibility. The strength of terrorists lies precisely in the fact that it only takes relatively modest means to shake a vast, coherent system. Even a highly localized terrorist action starts a chain reaction, sending shock waves through the entire tightly coupled system.

Individuals have been given considerable freedom and power to influence the community and contribute to the development. But individual freedom and influence can only be realized if there are clear rules and consistency in enforcing them.

If man were by himself, there would be no need of rules. But we are not alone on the widespread savannah anymore. It is the common thread running through human history that we are ever closer connected to each other - and our interaction would end in up in chaos without common rules.

Freedom and responsibility are not opposites: they are each other's precondition. Traffic rules are the classic illustration of this. Traffic wouldn't flow if we didn't have rules for which side of the road you can drive, or for who has the right of way. The individual must accept some interference with his autonomy - but this in turn is what ensures that everyone gains in freedom by being able to move quickly and safely.

In the future, it will not be sufficient to follow the relatively simple rules of the road, which we are currently learning to get a drivers license. We will have to surrender a lot more autonomy, if we want traffic to keep flowing. Traffic management systems in the increasingly crowded cities will need to know where we are and where we're going. Traffic flows will be managed, tolls collected, parking spaces booked ahead of arrival, and probably cars will be synchronized to drive semi-automatically in convoys. Pedestrians won't be allowed to just walk around without making themselves known to the system. As a driver you are enmeshed in a dense, coherent system that is often pushed to the limit.

Our freedom is contingent. When we are together with others and if we want to avoid gridlock, the individual must adhere to the common rules - and those rules will be more extensive and more detailed, the larger and tighter coupled the system becomes.

The dilemma of monitoring

The demand for more openness as our interactions becomes closer, applies to our interactions with machines as well. From sunrise to sunset we are assisted by computers that are rapidly becoming smarter and better at understanding our needs.

We cannot expect the system to adapt and evolve and to deal with us individually and intelligently if we plug the ears and blindfold the system. The more computers know about us, and the better they get to share that knowledge with each other, the better they can adapt their behavior to support us, efficiently and accurately.

That is why monitoring is a dilemma: It offers us new opportunities, but we feel that the price is our freedom.

If you want your GPS to help find your way, you must necessarily tell it where you are and where you're going. Similarly, mobile phone systems have to know where all the phones are located in order to make the connections between them.

We all have antivirus software on our computers that scans our mail for suspicious content. Probably our ISP and the provider of our e-mail account do so too. This may sound alarming; that there are programs, which read through everything that we receive - but that is a precondition if the computer should be able to ward off attacks.

We are equipping society with an infrastructure that increasingly demands that we make our selves known if we want to participate in the community. Before, the norm was that we were anonymous, unless we were explicitly recorded. The new standard will be that we are known in pretty much all the contexts we engage in, unless we specifically take steps to be anonymous. We have freedom, but it is in full, public view. One should not expect not to be seen.

The late Andy Warhol predicted that in the future, everyone would be famous for 15 minutes. The revised forecast is that everyone in the future will be anonymous for 15 minutes.

My data, your data, our data

The degree of transparency in society is closely linked to the balance between the individual and the community. The tighter the community, the more we inevitably know about each other. If you see your own interests as coinciding with those of the community, then you will be more open and similarly, you will expect more openness from others to make the interaction as intelligent and effective as possible.

The classic argument in defense of surveillance is that if you have nothing to hide, then you have nothing to fear. And yes, if indeed we were a single global organism, in which we all had shared interests and everyone did their best to optimize the interactions for the common good, then transparency and monitoring would be no problem. In fact, secrecy and confidentiality would be obstacles that made the joint interaction and development less efficient.

The limit for privacy runs exactly where the community ceases. Currently, the balance is shifting, from *me* in the direction of *we*, and similarly the influence of the community moves even further into the individual sphere. As that happens, for every step toward stronger connectivity, we will feel that the limits of our previous notion of privacy are exceeded.

The reason is that we are playing several games simultaneously. At a very general level, we will increasingly be playing the common game of making humanity survive and flourish. In the overall game, we have shared interests, but below it there are many other smaller, more personal games, which involve individual gains, negotiations and tactics. And in those games it is important to be able to manage ones information - of course.

Furthermore, it is certainly conceivable that those who collect information, are not only keeping the community's interest in mind, but also use the data to promote their own interests.

Monitoring is a power struggle. Some can see more than others, and they can use this to control or manipulate others. In that sense, "monitoring" is different than "transparency."

Transparency in the service of democracy

Monitoring is typically unidirectional, a kind of reverse broadcasting, in which a central agency keeps track of the masses and has exclusive access to create and interpret the data that's collected.

This top-down type of monitoring is challenged, however, because increasingly we

will all have the opportunity to gather and share information. Besides the state and public sectors' collection of key data for administration and security, there is a wealth of opportunities for ordinary consumers and engaged citizens to gain insight, for instance into the ways in which large corporations behave, or what our politicians are doing behind the scenes.

There are numerous examples of how grassroots organizations use the Internet to expose corruption, pollution or fraud and thereby help to have it changed. One of them is *Farmsubsidy.org*, a website, which for each EU country shows who are the largest recipients of farm subsidies - and for instance makes it easy to see that it is typically large, international corporations and landowners who receive considerable subsidies. When *Farmsubsidy.org* started, this information was not freely available, but as journalists and activists in many countries gradually managed to compile the lists of recipients, it created a lot of pressure for making the information public.

Globalvoices.org is another example. Here you can keep up with the undercurrent of political underground media, read blog posts and watch footage from the world's hotspots. When there are street battles in Iran, War in Palestine, uprising in Burma or demonstrations at the most recent summit, the material on *Global Voices* often offers a far more direct insight into the situation on the street than the professional media provide.

It is also telling that when you see footage of street fights and conflicts, a large proportion of the participants seem to be standing with a mobile phone or digital camera to document the event. It is not only authorities and companies that are surveying consumers and citizens - we can also look back at them. Transparency means that those in powers know that they can be held accountable by the small. It is clearly a disciplining factor, that the media almost daily publishes revealing and scandalous stories about politicians or companies who believed that their dubious practices could remain out of sight.

Nevertheless, it would be naive to believe that transparency makes us all equal. Since 9 / 11 authorities around the world have acquired far greater powers to monitor citizens. Enormous databases have been built, tracking our use of payment cards, telephones and the Internet, while millions have had their fingerprints and DNA sampled.

Technically, the prerequisites for a quite extreme surveillance state are largely in place. The challenge is to balance the interests of the community in protecting itself against terrorists, criminals and other harmful elements against the interests of civil liberty and the danger that the development of society is stifled by control, fear and self-censorship.

When we are confronted with the misdeeds of terrorist organizations or international network of pedophiles, it is tempting and relatively easy for politicians to turn up the surveillance. Every time there's a new threat or drama, the level of control gets another twist upwards.

It is much harder to ease the rules again. Terror laws and emergency measures have a tendency to become permanent, and there is a risk of "leaking", so the new data collected in the name of fighting terrorism, begin to become a normal tool to reveal petty offenses. Too many closed hearings, special terrorist clauses, secret indictments and extensive access to personal data, however, undermine the rule of law and the basic culture of trust in society.

What happens to the information about me?

The collection of personal data by *private* companies is arguable even more detailed. Like the states' registration of citizens, the gathering of customer insights by businesses is accelerating - and for good reasons: Businesses are increasingly competing on their ability to understand consumer needs as accurately as possible - partly in order to provide better service, partly to increase sales. It can hardly have escaped anyone's attention that advertising funds a very large part of the services on the Internet. The better targeted the advertising can be made, the more effective and valuable it is, and our use of the Internet and the information we leave about ourselves there, has led to a quantum leap in the ability to analyze consumers in detail.

It is downright extreme how much Google knows about each of us. Everything we have searched for, the maps we've used, the mails we have sent through Gmail, the videos we've seen on YouTube ... And what Google hasn't registered, Facebook has. There are over half a billion users of Facebook, and many of them have created a profile that gives an intimate insight into their social lives and emotions - complete with photos. In addition, we use services like Amazon, iTunes and eBay, who get to know our cultural preferences, and the online banks, which know our financial situation in detail. It is already very extensive, what a handful of companies know about us, and the level of detail will only increase as we move forward - for example when it all gets combined with our geographic location.

The problem is not so much that data are collected, or that they are used as a basis for ads or intelligent, personalized services. It is rather, that the users of Web services have very little control over what is recorded, and where it ends up. As ordinary users, we know almost nothing about what companies use the information for, how long they store the data, who gets access to them, etc.

We all know the feeling of acting blindly when filling out your name on a website in order to access an article, register some software or a to activate the support for a new device. There are lots of transactions, which imply that you give companies access to your computer without having the faintest idea what they actually install or intercept in terms of information.

Very few of us have the time or are sufficiently interested to actually read the license agreements that you must click OK on - whether it's to become a member of Facebook, buy a plane ticket or download software and music. We just want to get on with our lives.

Should you, however, make the effort to read the agreement, you will quickly realize that it is a document written with all the ingenuity a major U.S. lawyer can mobilize. It is usually written in absolute attorney-speak and loaded with general terms, reservations and disclaimers. I can only recommend trying it once. It is an interesting experience to read, black on white, how conscious companies are of securing their right to use the data in any way possible. But exactly how they actually intend to use them is typically impossible to infer from the text.

Nevertheless, we usually choose to trust that they behave nicely and at least stay within the law. We have to; otherwise we will not get access. In reality, we have no choice. If we don't allow Google to record our queries, or if we do not have a Facebook account - let alone a bank account - we cannot really participate fully in the normal culture of society.

One problem with the private registration is that the users and the providers of a service sometimes have opposite interests. A person, who uses Facebook, wants to be social. You are willing to share very personal information because it's part of having a conversation and relationship with your online acquaintances. For users, Facebook is a private space that they share with the people they trust.

For Facebook itself, the service is a business and it makes money by providing advertisers with access and as accurate knowledge about users as possible. Therefore, it's in Facebook's interest to push for making the data about users as open as possible - of course referring to a philosophy in which openness makes it possible to deliver better and more personalized service for users.

We are constantly *on*

Of course most personal information remains proprietary and confidential. But very personal information *can* unexpectedly become public, or it may turn out that it is being used in ways that are considerably more revealing than what those who let the data about them be collected, had imagined when it was recorded. Sensitive information has a tendency to leak. Revealing and inconvenient records can suddenly re-appear even after many years - at full strength.

If one makes a bit of noise - as a politician or "celebrity" - you risk getting caught in a particularly intense spotlight and that your privacy and past gets raided and exhibited. As the systems to filter and analyze get stronger and smarter, this type of pervasive transparency will be a risk that many more of us must learn to live with.

People's memories fade with the years, but the network does not forget the past. We can very easily end up being judged as a person we no longer are, by values that are quite different from when we were.

Unless someone actively deletes them, our data will keep lying around out there somewhere. Even if one tries to correct information that is false or which you don't want others to see, you can't be too sure that they really are gone. It's like stirring cream into coffee, once the information is out there, it's almost impossible to remove them again.

We will be *on* all the time – and we need to get used to that. We are – so to speak – acting on a stage where others can see us. But we don't know who is watching, how many are in the audience, or when they are looking. Some day, when someone pieces the information about us together, we can't know what context we will be shown in, or what role we will play.

It may sound rather unnerving but actually one could easily conjure up more, far more extensive surveillance scenarios that might very well become real. For some of us it will have concrete and unpleasant consequences that monitoring becomes so intense – for instance for lots of Facebook users, who haven't quite yet realized that their inner feelings, wild partying documented in photos might also be studied, years from now, by business associates, employers, suspicious boyfriends or even the police.

For most of us the effects are psychological rather than practical. We will know more about others and we will know that they know more about us. It can lead to a paranoid culture in which nobody dares do anything that falls outside the range of normal behavior. Conversely, one might hope that transparency will both make us both more accountable as well as more understanding of the obvious fact that we all have our

quirks.

A transparent society is not necessarily equal for all. Some have access to more information than others and there is a risk that they use their knowledge to manipulate others in unfair ways. And that undermines the community. If we are exposed and held accountable to values we don't share and to standards we couldn't predict would matter, we will lose confidence in the benefits of openness and consequently try to hold back information.

It's all in the cloud

The dilemma of monitoring brings us back to the recurring problem: Where is the border between mine and ours; between the individual and the community?

It seems that in the future a large part of our data will be stored in *the cloud*. The idea of cloud computing is that each individual user or each individual enterprise does not need to have the capacity to store and manipulate lots of data. Instead they leave it to companies that provide computing power as needed – like an electric utility company. Basically the data can be stored anywhere in the world - it's simply out in the Cloud, somewhere. We know it already from e-mail, or if we are using services like Flickr to store and share our photos online: Where is our e-mail? Where is the server with my photos? We don't really know, and it doesn't really matter.

Technically it's all stored on the same big server. In the cloud, deeply personal and sensitive data is only separated from the banal and general information through the way they are classified.

It is an important point: that our data is collected and can be accessed from anywhere, but we can set the conditions for admission and their degree of openness.

It requires a slightly technically detailed example to explain: Google has developed an alternative to Microsoft's dominant Office suite (the one with Word, Excel, PowerPoint and Outlook). It's called Google Docs and it offers virtually the same functions as Microsoft Office. The main difference is that you use Google Docs through a browser. You must be online for it to work, because the documents and programs reside in the cloud. Among other things, this has the advantage that you can access your documents and work on them from any computer on the Internet. By the same token, many different people can be working together on the same document. There is one small detail in the Google Docs interface, which gives an indication of how we might deal with data in the future. When you save your work, you have two choices: *Save*, and *Share*. If you press Save, it will be filed so only you can see it - just like you are used to in Word. If instead you chose to Share, the document will be made public. You can choose from a variety of ways and levels of sharing: with specific individuals or with different groups of people. You can select who you want to share the document with, who are allowed to make changes, and you can choose whether they in turn are allowed to invite more people to the group, which has access to the document. Finally, with a few key commands, you can upload the document to be published on your website.

This is a very different approach than the traditional closed model, in which a user sits with his own information and private projects on his personal computer.

The principle is echoed in many other types of Web services - whether you upload

pictures, videos, personal profiles, or medical information: It all goes into the cloud. The only difference in how public they are is the degree of access you assign to them. We are all accessing information on the same hard drive - but some have more access than others. The crucial questions are who gets to look, what are the criteria for others to access the data, and to which degree users themselves can control the access of others to their information.

Managing Presence - an essential competence

The Institute For The Future in Palo Alto use a phrase that accurately expresses what it's all about: *Managing Presence*.

Being able to manage ones presence in many different contexts will become a critical skill in the future - it's almost a kind of personal hygiene. Just as we are aware of our dress and physical appearance to others, we must learn to deal with how we appear *virtually* - and we will demand to have the tools to do it in an easy and simple manner.

Craig Mundie, Microsoft's senior technical manager, has put it like this:

"You have to realize that the world is going to be a sea of data, and the real question related to privacy is going to be, how does the user get to specify what they think their ownership rights are in that data - no matter who collected it.

People can certainly speculate that there are evil ways to use and exploit data, and the question I think will become: how can we find a manageable way for people to declare their intent about each class of data and each class of service that they subscribe to?"

Actually, managing presence shouldn't be a defensive activity. We must protect ourselves, yes, but for the most part we don't dress to blend in with the crowd, but rather to send a signal about who we are and what type of interaction we are prepared for. To manage our digital appearance is something to be learned, and to the extent that we have mastered the art of controlling the way we are looking to others, managing presence can be an extremely useful tool when we interact over the net.

There is a great difference between being watched and publishing your own data.

If people are confident and feel they have control over the process, they will let their guards down. On the social websites users blurt out the most intimate aspects of their lives. Websites and blogs are elaborate showcases for their owners. They want to be seen, they want to be known by others, they want to inject their lives and thoughts into the rest of the interaction in the community.

There are plenty of people who virtually live online. There are Facebook fanatics, there are those who twitter incessantly, there are avid bloggers, and some that spend their time in fantasy worlds like World of Warcraft and Second Life - there are even those who seemingly manage to be active on all platforms simultaneously.

It may seem unwise and revealing when people put so much of themselves on display, but conversely, it is precisely because they contribute so much that they achieve a position and make their community lively and interesting.

We are back to *letting go*. We must learn to dare to surrender to the community. Being visible and being held accountable sounds intimidating, but actually you can be

held accountable both positively and negatively - as long as the good we do, gets noticed, too.

Transparency can control us, or it can liberate us. If the reality is that we are always on, we might as well act offensively and make our views and actions known rather than trying to hide in the bland and formally correct. Only then can we achieve a community that is about commitment and diversity rather than a fearful community built around the standards, everyone assumes that everyone else think is normal.