



*Ethics at the Root of Privacy and as the Future of Data Protection*

*Address given at event hosted by Berkman Center for Internet and Society at Harvard University and the MIT Internet Policy Initiative and the MIT Media Lab*

*19 April 2016*

*Giovanni Buttarelli*

It's a huge pleasure to be here.

Let me thank Amy Zhang, Malavika Jayaram, Taylor Reynolds and Urs Gasser and their colleagues at MIT and Berkman for arranging this talk on a topic as important as it is fascinating.

This is an august academic institution, and I am addressing a group of brilliant scholars. I know that every day you drill deep into the assumptions of everyday life and question their validity.

So I want in the next 20 minutes to get under the surface of the law of privacy and data protection.

I want to argue that ethical concerns are the essential unpinning of the right to privacy, and that they are the future of how society will seek to govern how personal information is processed.

In the digital age, privacy, according to some billionaires - as well as the occasional Harvard academic - is dead.

This is of course nonsense.

Regardless of how indiscreet you might be on social media

- offline you still take steps to preserve a part of your life separate from the public arena;
- while online from virtual private networks to ad blockers to Snapchat, people find techniques to conceal their tracks.

That is privacy.

Yes, the internet disrupts and transforms norms of human behaviour.

But there is no evidence that it has fundamentally disrupted our values as a society.

In the EU there is a fundamental right to privacy.

In the US, you may not use the language of fundamental rights, but the same principle is there in the Constitution. And the notion of a negative right, the freedom to be left alone, was formulated in the United States in an article in the Harvard Law Review.

Of course in the EU we have a separate fundamental right: the right to the protection of personal information.

Unlike privacy, this is a positive right – it means that as an individual, you have the right to expect that information about you is handled in a respectful way.

Now when I started working in this area, data protection was still largely about paper documents stored in filing cabinets.

Nevertheless the EU broke new ground in 1995 when it passed a comprehensive law regulating how personal data should be processed across the internal market of (then) 15 member states and 373 million people.

Ten, even five, years ago, the data protection was a still niche of the EU legal system, and a marginal political issue.

But thanks to pressure from independent data protection authorities and from civil society and academics, the European Commission took up the cause of modernising the directive to be more relevant for the age of instantaneous communication, ubiquitous data and potential indefinite storage of those data.

Last week, the EU – now 28 member states with a population of 508 million – adopted the GDPR.

This is an historic development.

In a globalised economy, it affects every country in the world which trades with the EU, whether offering services to people in the EU or monitoring their behaviour.

The regulation will be directly applicable in the whole European Union.

It's a long document, very detailed and prescriptive.

But it introduces accountability – which is a novel concept in EU law.

Accountability requires organisations to put in place whatever measures are needed to comply and to demonstrate compliance with the principles of data protection. How they do it is largely a question for those organisations.

This is the one way in which data protection in the EU is emulating antitrust enforcement.

Another major change relates to the enforcement mechanism. In Europe, independent data protection authorities play an important role. Each EU Member State has such an authority, with wide responsibilities in the area.

I head the independent European authority responsible for data protection at the EU level.

The new regulation must further strengthen this enforcement mechanism. All authorities will have the power to impose administrative fines up to 20 million Euros or 4% of the annual worldwide turnover of a company, whichever is higher.

Those numbers make data protection a board-level issue.

And that is a second way in which data protection has come to resemble antitrust.

Europe may be a laggard in some areas. But in data protection law, it is undisputedly in the global vanguard. We know that from the facts that over a hundred countries around the world, most now outside Europe, have passed data protection laws, and that most of them have based them on the EU approach.

But let's be honest. The 1995 Directive did not really affect the evolution of the internet. It did not prevent surveillance becoming, according to Bruce Schneier and others, the internet's prevailing business model.

The law has its limitations.

That is why I am so interested in the ethical dimension of the law in this area.

Ethics, the idea that something is right or wrong, is more universal than the typically western notions of privacy and data protection.

Ethics both informs the laws which are passed, and goes beyond them.

So is it possible that a company processing information complies with the letter of the law, yet behaves unethically?

How can such a question be analysed? Are regulators capable of analysing such a question?

For me, big data is the perfect illustration of this question.

Big data is a phenomenon whereby vast data sets from various sources are combined and analysed using powerful computers to draw inferences about, and to influence, behaviour – especially human behaviour.

Much talk about big data is hyperbole and marketing.

But I have just spent the morning seeing some of the outstanding work of the Media Lab in MIT, where they are exploring how massive volumes of data diversely sourced can be harnessed for productive purposes

Big data is just one example of how personal data is driving technologies and practices in the marketplace and public sphere. Artificial intelligence, virtual reality and robotics are areas which are approaching on the horizon.

The tech giants which have built their empires on big data are now turning their focus to these new technologies. And these technologies raise profound questions not only about human rights, but also about what it is to be human.

There is no doubt that we need innovative thinking and to explore the ethical dimensions of our digital society. Big data delivers significant benefits for society and also for individuals. Big data analytics has the potential of improving policies in a wide range of areas, in a substantive way.

But the question is who benefits. Is it society at large, or just a few individuals?

Obviously, all data processing potentially affects privacy. In a big data environment innocent information from various sources can be combined and can deliver precise pictures of the behaviour of individuals.

Moreover, the business models of internet companies - as I have mentioned - tend to be based on the monitoring of individuals. It is the aim of these companies to sketch precise pictures, and to monetise these pictures and give access to people who fit these pictures.

Data on individual behaviour have become an important economic asset.

Privacy has almost become a commodity.

In my opinion of September 2015, entitled "Towards a new digital ethics", I outlined four main lines of such an ethical approach.

First, privacy and data protection are increasingly important for protection of human dignity. Privacy and data protection are enshrined in the EU Treaties and in the EU Charter of Fundamental Rights. They enable individuals to develop their own personalities, to lead independent lives, to innovate and to exercise other rights and freedoms. These values should be leading on the internet.

Second, technology should not dictate our values and rights. We should consider the impact of trends in a data driven society, on dignity, the individual freedom and the functioning of democracy

Third, as I already said, in today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing.

Fourth, big data has engineering, philosophical, legal and moral implications. These implications should be part of our reflection on the digital society.

The Ethics Advisory Group which I have established this year will look at classical approaches to regulation of personal data processing, and test them against the emerging technologies I have mentioned.

We will be engaging anthropologists, philosophers, social and computer scientists in what I hope will be a transparent global conversation.

We are looking at some fundamental questions.

Firstly: What does privacy mean in a society characterised by massive data sharing? As we all know, views on privacy are changing, if only because many people share a lot of personal information on social networks. But not all people wish to share personal information and the people that are active on social networks are selective in the information they do share.

We need to revise our notion of privacy against this backdrop.

Secondly: To what extent should ethical considerations influence the development of new technologies? For me, there is no dichotomy between ethics and innovation. Rather, ethical considerations should determine the direction of innovation. If we, from the start, build in an ethical assessment in the development of new significant innovations, we would not only encourage progress, but also ensure a society which is built on human values.

Thirdly, is ethics an alternative to the law or complementary to the law? I am convinced that responsible organisations should be driven by ethical considerations. As I already said, for me it is not enough for companies just to comply with legal requirements.

In our area, we talk a lot about accountability of data controllers, a notion which goes beyond compliance. We need to understand better how ethical considerations relate to the law and the enforcement of the law.

I would like to give four examples of possible, promising avenues.

The first avenue could be an ethics committee for the digital society. We know ethics committees are taken for granted in various sectors of our society.

The medical sector is an obvious example.

Do we need ethics committees in the digital world?

This question raises a few fundamental further issues, such as the legitimacy of an ethical committee or the way such a committee would deal with different views on ethics in different parts of the world.

The second avenue would be to develop a policy on data ethics for businesses and governments, in addition to accountability mechanisms.

Again, however, who should be responsible for developing such a policy. Is this a task of governments, of other societal stakeholders, or both?

The third, more concrete, avenue would be to restore the data traceability in big data, by finding new ways to ensure controllers' accountability. If one considers the control of individuals over their personal information as a predominant ethical value, restoring traceability would be essential.

The last avenue I mention is the integration of an ethical dimension into the work of the independent data protection authorities.

The core business of these authorities is to enforce the law.

But of course, the duties of the authorities are wider. They also have the task of advising and of raising awareness on issues relating to data protection. In the future, I would like to see these authorities acting as the conscience of the digital world. But for that to happen they need to be conversant with technologies, and also with the ethical implications of those technologies.

In conclusion, let me remind you that the EU has just adopted a general data protection regulation which states, in its fourth recital, 'Data processing should be designed to serve mankind'.

This, I argue, is an ethical sentiment which can be shared from Chicago to Shanghai, from Copenhagen to Cape Town.

It's a global question, and I am very pleased to have the chance to bring it to Cambridge Massachusetts and the cutting edge of legal and technological academia.

Thank you for listening. I look forward to our discussion.