Eisenhower Fellowship – Multi-Nation Program 2016

Final Report

Rosalba Striani

The Fellowship has been a unique and invaluable occasion to meet key representatives of the US enforcement bodies, professionals and academic experts, concerning both competition and privacy related issues. Moreover, the program has represented a wonderful opportunity to travel through and learn about the U.S. during an unprecedented political moment. In addition, I must also be very thankful as the fellowship provided me with a priceless opportunity to learn about myself and reflect on my professional future and expectations. Finally, the relationship with other fellows was one of the most rewarding experiences, in terms of intercultural learning and building cross-cultural relationships.

At the outset, I had set three objectives for my fellowship. However, during the six weeks, I had the time to focus mainly on two of them: (i) understanding the American antitrust enforcement in relation to the interplay between the private and the public enforcement, in view of the upcoming implementation of the of "Damages Directive" in the European Union's Member States; (ii) understanding the peculiarities of the American enforcement and policy debate with regard to privacy rights, data protection and security issues, in the light of the current negotiations of the so called "Privacy Shield" concerning international data flows (a decision that will allow American companies collecting data in Europe to transfer and use those data in US).

The Fellowship has been a challenge as to the number of people I have met. On average, I met three persons a day, ranging from governmental representatives, judges, high-level private practitioners, experts from academia and civil liberties' associations. 75% of my meetings were satisfactory; however, I learned something also from the remaining 25% (that did not at the end contribute greatly to my objectives). At the beginning, I dedicated ca. 70% of my time to antitrust experts, while, in the course of fellowship my primary objective had changed to privacy.

Finally, since I have always been passionate about dance – I have danced for 15 years - my third objective was to look at the main challenges faced by dance companies in USA and how they develop programs to tackle socially marginalized people. I have therefore met with the U.S. Dance Association in DC and some dance companies in New York and Cambridge.

I. Antitrust enforcement

Before describing my project, I would like to give you a brief overview of what I have learnt in general on the antitrust enforcement in USA.

(i) Federal Authorities

Unlike in the USA, in Europe, we primarily rely on public enforcement, while private litigation still faces obstacles, mainly due to different approaches in the national legislations. In December 2014, the European Parliament and the Council of EU adopted a Directive with the aim to create a level playing field for the promotion of private litigation. This must be implemented – transposed into national law – by the end of 2016 in all Member States.

From my discussions during the fellowship, a consensus seemed to emerge that private litigation in America is essential not only to "compensate" victims of violations, but also to "deter" corporations from anticompetitive behavior (although this was not the original objective of

private actions). Private litigation is therefore essential to complement the public authorities enforcement.

In the US two federal agencies are leading the public enforcement action in the antitrust field: the Federal Trade Commission and the Department of Justice. Both have the power to pursue anti-competitive agreements and monopolization-related practices, as well as to assess mergers, however the DOJ has exclusive competence over criminal violations – such as price fixing cartels and bid riggings. Unlike in EU, where the competition authorities impose administrative fines as part of the administrative procedure, in US, the FTC and the DOJ may file a complaint before a court (in addition, the FTC has the alternative option to bring a complaint before the so called Administrative Judges) and request an injunction relief. In the majority of the cases, both authorities and the parties try to find an agreement, resulting in a consent order or consent decree.

Both authorities have discretionary power in choosing their area of intervention (driven primarily by the assessment of complaints and in some cases by political choices[1] –for the DOJ, mainly[2]), leaving enormous space for autonomous State actions and private litigation suits.

(i) State Attorneys General

States Attorneys General have their own antitrust (or equivalent) laws, which prohibit anticompetitive conduct and they bring actions when the case has no interstate effect. To avoid multiple investigations, coordination among Attorneys General is ensured by the National Association of Attorney General (NAAG) that meets every two weeks to discuss ongoing investigations and possible joint investigations. .

In the majority of the cases, State Attorneys General join, as co-plaintiffs, federal authorities' actions. Their main role is to seek monetary relief on behalf of their citizens (the so called "*parens patriae*" role) or to act themselves as victim of an antitrust violation. Their role is absolutely complementary to that played by the federal agencies. One example of this complementarity is to be seen in the recent the "e-book" case where Apple and 5 publishers were found to have engaged in an anticompetitive agreement to raise the price of the on-line books. In this case, while the DOJ focused its action on the request for an injunction relief, private plaintiffs and a coalition of State Attorneys General requested monetary relief for the victims of the violation.

It is to be noted, however, that the system is structured in a way that private class actions work also in the absence of the federal government intervention.

(ii) Private litigation

The sum of different **factors makes the private litigation successful in USA:** (i) the possibility to bring a "class" action, which ensures a large number of participants and a correspondent recovery; (ii) the opt-out system of the class, which does not require the victim to express the desire to join the class (they are automatically in, unless they explicitly opt-out); (ii) the contingency fee-based contract with the plaintiff lawyers who will receive a final sum of money only in case of victory; (ii) the provision of law on treble damages that the defendant will be required to pay in case of a confirmed anticompetitive conduct by the judiciary.

---

[1] In general terms, historically Republicans, unlike Democrats, have been friendlier vis-a-vis business and therefore less interventionist.

[2] In some cases, the DOJ can ask the President or inform him before taking an action.

Despite the different rules, on which private litigation procedure is grounded in USA[3], I noticed curiosity, especially from lawyers, but also from academia and judges, regarding the implementations of the new European rules.

- **Next steps**

My idea is to try to bring the US experience into EU developing practice and focus on the main factors that are likely to influence private enforcement, not limited to legislation and procedures but also to behaviors.

America has 40 years more of practical experience on private litigation in antitrust from which we can learn. I would like to establish a dialogue with the American professionals I have met, involving them in a series of workshops/seminars with European judges/governmental official/ lawyers/experts from academia to discuss over the main procedural, strategic and substantial issues. **Among these:** (i) the risk assessment that a corporations have to make before deciding to bring a suit against their supplier; (ii) the antitrust recovery options: individual suit, class action, direct or indirect purchaser, global recovery strategy and settlements; (ii) how to make best use of economic expert especially in the quantification of the damages; (iii) how to make the discovery efficient: due to asymmetry of information it is important to know the right technique to ask for the right documents as well as how to approach the witnesses pre-trial; (iv) the mechanism put in place to protect confidential information; (v) how to solve the issue of forum shopping and the need to avoid parallel actions (create a mechanism mirroring the US multidistrict litigation committee); the strategy and the technique both from the plaintiff and the defendant side to strike good settlement.

As I have said above, although the primary aim of private litigation in US was to compensate victims of antitrust violations, it turned to be essential to deter future anticompetitive behaviors.

Privacy

Today, when business and innovation are both grounded on the collection and use of data, privacy and data security issues are under particular attention of civil liberties organizations, corporations, policy makers, legislators, intelligence community and technologists. I therefore, used my fellowship to understand the US legislative framework on the protection of privacy and the enforcement over security issues and to look into the main challenges faced by corporations operating on the two different sides of the Atlantic. In the new digital economy, with cross-border data flows never more critical to the success of companies, industry must constantly understand and adapt to frequent shifts in international trade policy and individual country-specific data protection policy. Frequently, these shifts are not synchronous with one another, making it challenging for companies and counsel to navigate a clear path.

In this scenario, moreover, I have used the fellowship to look at the interplay between privacy and competition. In particular, at whether corporations and consumers use and look at privacy policies as a non-price element for competition.

- **The "right of privacy" in the U.S.**

In Europe, privacy is a constitutional right[4]. To clarify the rights and obligations related to the protection of privacy we have recently adopted a new Regulation (GDPR) which introduces very

[3] We have not foreseen the possibility for treble damages. Moreover, we urge to adopt an opt-in system of class action and in some Member States, contingency fees are prohibited.

[4] Art. 8 of the European Chart of Fundamental rights.

detailed and prescriptive provisions for firms in the world which offer services in EU. This piece of legislation will enter into force in late 2018.

In the USA, there is no explicit specific constitutional protection of the right to privacy, although some Sates do protect privacy in their own Constitution, as the State of California. At federal level, the FTC ACT (the general consumer protection act) is the main tool used by the FTC to detect "deceptive" and "unfair" practice. Moreover, sectorial laws are in force to protect the privacy of targeted consumers or consumers in specific industries (e.g. financial, healthcare, children).

Following the Snowden revelations, the American government has been urged by civil liberties associations to adopt a privacy Bill of rights. Despite the attempt made by the Obama Administration, which ended up in non-enforceable guidelines, it seems very unlikely that the American Congress would pass such an act in the near future, mainly because corporations look at a possible comprehensive legal framework on privacy as a threat for the innovation.

In this scenario, whereas the FTC is trying to set privacy protection guidance, through its enforcement, it is left to the corporations to figure out, "on general ethical rules" what kind of privacy policy would best suit their company (so called "privacy by design"). The FTC enforcement is generally perceived as not-enough-deterrent (the FTC has not fining power unless companies violate its orders). The perception is different with regard to specific regulated sectors and to some State enforcement actions. The States of California for example is among those that, together with Illinois and Massachusetts, have serious deterrent powers. Under the California "unlawful and unfair" act (UUDAP), the Attorney General can impose a fine of 2500 dollars per violation (meaning p. each app downloaded or per each day the violation occurred) on all companies providing service in California (not only those based in California). As for the private enforcement, despite the increasing number of class actions brought for privacy violation, there is still an issue of "standing" based on the need to show the "harm" caused by the violation of the "privacy". This issue is currently under scrutiny of the Supreme Court (*Spokeo case*)and its outcome might affect in a way or another the deterrent effect of private litigation in the field of privacy.

From the corporations point of view the US legislative framework even if seen as less regulatory than the European one it is also perceived as particularly burdensome due to the number of State and Federal laws (for example, in the U.S. some data breach notification requirements are part of federal laws regulating certain sectors, e.g., healthcare and financial services, and there are more than 46 state laws imposing notification obligations on organizations that discover a breach of security involving personal information). Moreover, companies that want to operate in Europe must comply with the GDPR rules and those that want to transfer data from Europe to US must comply with the provisions of the so-called Privacy Shields.

Rules are different and there is a strong request, from the professional world, toward more dialogue between the EU and the US government to converge.

- **<u>The debate on "security" issues</u>**

The post-Snowden era has, from one side increased the awareness of consumers on the use that corporations and governments might do with their data. On the other hand, from the law enforcers and the intelligence community there is an increasing request to access to those data to prevent, detect and fight crimes/threat to national security.

From a security point of view, if strict encryption policies (protecting individual sensitive data) represent an obstacle to get information from governments and intelligence communities, corporations (such as Apple and Microsoft) have stressed that undermining devices to provide the

government with access would undermine the security of the entire system, opening backdoors to cybercrimes.

There is not a clear answer yet on how to balance those needs. Issues of "national security" remain in the exclusive competence of each state. However, despite the difficulty to converge on such a complex and sensitive subject, we should build on a common assumption: there are constant and innumerable attacks by criminals on all online secure systems and a starting point to fight them should be a more intense dialogue among security experts, law enforcers and intelligence community.

- **The interplay between privacy competition**

Considering the evolution of markets, business models and competition in the big data as well as taking into account the consumers behaviors, I have explored whether "privacy policies" represent or will represent a "non-price" element for corporations to compete, in the light of the antitrust and merger legislative frameworks. This interplay, despite recognized as extremely relevant, has not been fully explored. In 2008, the FTC Commissioner, Pamela Harbour, in the context of the Google/DoubleClick merger, dissented from the approval of the merger, as the market analysis had not looked at the collection of data as a non-price element for competition: the mergers might have had the ability to reduce the security of consumers. However, so far competition enforcers have been reluctant to use traditional competition enforcement tools to look at the effect on privacy.

I believe, however, that competition enforcement might represent an efficient tool to protect robust privacy policies. Merger law for example can be used to look at a potential merger between two social networks where the locked in effect on consumers (in terms of the "indispensability" for them to be part of that network) might lead them to accept any kind of privacy policy, even if less protective.

From the consumers' perspective, however, there are no studies yet assessing the effect of privacy policies on consumers' choices. Prof. Florencia Marotta whom I met at NYU, has recently conducted a study on the attention that consumers dedicate to read privacy policies. The results showed that the majority of consumers do not read privacy policies, mainly because of the complexity and long structure of the contracts. However, the new rules imposed by the GDPR on "transparency" obligations might change this result in the future. Moreover, it would also be necessary to distinguish the category of consumers and their choices in different markets: the type of business might influence differently their behavior (e.g., in the financial or healthcare markets consumers might pay more attention to the protection and the use of their data).

We also see how recently companies have marketed their strict privacy and security policies against law enforcers' requests (see Apple and Microsoft cases). This might be an indicator of a possible change in the future of market factors. Moreover, business models might be affected by the need to provide robust security policies: what if the security requirement would not allow companies to collect any more data that are essential to online advertising?

In a developing digital age where we talk about "internet of things" and "robotics" and where consumers behavior is changing, we could not ignore the impact that privacy and security issues are playing on competition and vice-versa. My intention is to work on stimulate this debate promoting a stronger dialogue between privacy and competition experts.

- **Next steps**

While looking at each specific issue concerning privacy and data protection in US, I became aware of the essential interaction between human rights, technology and security issues. During

my fellowship, I visited several Universities (Harvard, Stanford, Berkeley, NYU) where specific centers have been set up to approach the aforementioned, in a multidisciplinary way. Unlike in the US, Europe, despite facing the same challenges, is taken a more sectorial and compartmentalized approach.

My idea is to promote the setting up of a research center, which – as main objective – would look at the interplay among the several disciplines related to big data. It would have the task to study the interplay between those disciplines, stimulate the debate and at the same time have an advocacy role.

During my trip, I had the chance to meet with the European Data Protection Supervisor (EDPS) that is very active on those issues and is committed to international solutions. He was very interested in the fellowship and brought me along with him to meet MIT experts. I intend to contact him, on my return in Europe, to propose to establish the research center at the premises of the EDPS.

The center could become a reference point for lawyers, business persons, academia representatives, for their everyday activities in Europe. Moreover, I have experienced a general need from American professionals, to have a point of reference in Europe and engage in common projects. This will also be a task that the center might accomplish.

Conclusion

All the above it is one of the results of a long reflection built up on the interesting meetings I had in the course of the fellowship. The fellowship as I said at the beginning was much more than that. In few words, if I could refer to “cooperation”, “integration”, “innovation” and “security” as the values underling my professional goals. I would refer to “friendship”, “self-confidence” and “equality” as the values I got in return from a personal point of view.

Thank you all for this unique and incredible experience. I will keep myself committed.