

BTO - Meeting Carl Buhr (Cab Gabriel) with Mastercard on AI, ePrivacy and Women in Digital

BTO: Mastercard visit Cabinet Gabriel on Artificial Intelligence, ePrivacy and Women in Digital.

Participants:

External:

[REDACTED] Government Affairs & Public Policy Europe
[REDACTED], Account Management, Banco Santander
[REDACTED] Privacy & Data Protection, Mastercard

Internal:

Carl-Christian BUHR (Cabinet Gabriel), [REDACTED], (CNECT A1)

Objective of the meeting :

Discuss ePrivacy & GDPR, AI and Women in Digital

Executive summary:

Mastercard (MC) presented its activity, in particular switching services, and stressed the privacy by design approach in the fraud prevention services they develop, some of them based on AI. MC expressed concerns about

the need to provide consent in the current draft e-privacy regulation, and MC recommends exempting from this requirement companies that process data for the sole purpose of fraud prevention and monitoring, and authentication. This is critical to prevent fraud.

MC develops AI-based tools to ensure that ethical principles are respected (accountability, fairness, security by design, transparency and explainability).

MC is also very active to promote women in digital, and have a number of substantial initiatives already.

Finally MC has started to collaborate with other companies on cybersecurity.

Points discussed:

1. Information about Mastercard

MC considers being a tech company relatively small (<14000 people):

- Since 2006 - private company, taking care of switching transactions (between the bank of the buyer and the bank of the seller) for 25k bank customers.
- Explanation regarding the news MC releasing information to Google <https://www.bbc.co.uk/news/technology-45368040>
- Potential for B2G: Such aggregated information is interesting for governments to develop policies (eg: a city developing a tourism strategy is interested in the trends of the buyers, same for smart city strategy development) or companies to develop their business. Interesting Business to Government example.

- MC provides fraud detection tool to the banks, based on machine learning, to detect suspicious patterns of bank account usage.

1. Fraud prevention in switching transaction - link to ePrivacy/GDPR (additional information in annex)

- Off-line payment are gradually replaced by on-line payment (no card), but on-line payments are much more fragile. Hopefully the revised Payment Service Directive requires security measures.
- MC uses biometrics authentication to combat the increased fraud (such as identity fraud), and apply privacy by design in the use of biometrics (store template - no biometric information, and information kept on the device, not transmitted, no excessive retention of information - only go/no go decision provided)
- Issue in the draft ePrivacy regulation requiring consent for use of information: the metadata used for security/authentication includes location and device information (new device/ used for a long time by this user, etc.). Lawyers take a conservative approach claiming that users should be asked to give consent to access such information in all cases.

EC answer: MC should not be concerned as it is not an electronic communication service provider (e.g., MC, the banks, and the users are not ESP).

GDPR includes in the recitals exemption to require explicit consent for fraud prevention but ePrivacy does not include such exception. One issue is when does GDPR(data) vs ePrivacy applies (device).

ePrivacy regulation needs simplifications, especially for smaller companies.

2. MC & AI

MC applies privacy by design, in line with GDPR, based on AI, involving human supervision, to establish

- accountability, fairness (ensuring repeatability, consistency, possibility to contest (no automatic decision)), security by design
- transparency and explainability (no technical details were provided - MC offered to send an expert to provide more information)

The EC encourages MC to channel their input to the HLEG, and share their experience.

MC would appreciate if the guidelines of the HLEG could be sector (financial/ security/...) specific, stressing the importance to make sure that the guidelines are in line with GDPR / liability directive...

3. MC & "Women in Digital" (more information to be provided afterwards)

Diversity very important for MC, especially given that many financial decisions are made by women. Some concrete actions: ensure same salary for men and women, generous parental leaves for men and women, pilot project in the UK bringing back women after taking care of kids, parents, which is challenging, especially in the fast moving sector of IT.

MC also has a program to attract young kids (especially girls) to digital careers, in 17 countries . For instance one programme involves 30.000

children from 9 to 11 with schools, open market initiative
(London transport museum), Barcelona Mobile World Congress.
MC works with other groups (American chamber of commerce in various
countries to cooperate on the topic with US companies in that country),
targeting kids, women, mentoring across companies.

MC works on financial inclusion, addressing the 70 million women in Europe
who do not have bank account/cards/..., using technology (they usually
have a smart phone)

MC also works on financial inclusion in Africa (Joint Venture with B. Gates), also works with the UN.

Some examples: in some countries in Africa, without ID card, MC developed
pre-paid card, recognised also as ID now. MC also develops digital
accounts (without a bank - just an app) around the globe.

4. MC invests heavily in cybersecurity

They have millions of cyberattacks every day, and their service is really to secure transaction. They
are now connecting to companies (telcos, banks, merchants, ...) to share information and be more
efficient against such attacks.

The EC welcomes such collaboration.

ANNEX: additional documents on ePrivacy regulation and Mastercard Business model