Comparing Commercial and Political Microtargeting

Regulatory Implications based on an Interdisciplinary Analysis

Max von Grafenstein
Jessica Schmeiss

Introduction

Big data, digital marketing technologies and new communication channels such as social media have significantly changed the way business (and politics) are done. Success now depends on an in depth understanding of what the consumer or voter wants and needs and the ability to develop a targeted marketing campaign to build a long-term relationship with that consumer or voter. Access to large datasets and the appropriate data-mining techniques to generate actionable insights from this data are crucial activities for microtargeting and building a successful marketing campaign. However, there is an increasing debate about the consequences caused by the use of such micro-targeting techniques in political campaigning for our democratic civil society. If there are, in particular, negative consequences, the question arises whether the use of micro-targeting for political campaigning requires further or other regulations than for the use of these techniques for commercial micro targeting.

An answer to the question of whether the usage of microtargeting techniques for political campaigning requires further or other regulations than for commercial microtargeting depends on the legal guarantees concerned. Typically, the debate refers, in both cases, to privacy or data protection. However, in this paper, we will demonstrate that there actually are different specific objects of protection concerned when microtargeting techniques are used, on the one hand, for commercial advertising purposes and, on the other hand, for political campaigning. These differences exist not only on the normative level regarding the specific objects of protection but also on the factual level with respect to the socio-technological circumstances. Therefore, we will demonstrate, in a first step, what these factual differences between both a commercial advertising and political campaigning context are. In a second step, we will assess which specific objects of legal protection are actually concerned by the use of microtargeting techniques in the context of political campaigning, in contrast to its use in the context of commercial advertising. On this basis, we will compare, in a fourth step, how the specific risks resulting from the use of these techniques in the political context are addressed by the regulators, on the one hand, in the USA, and on the other hand, in the EU, with a particular view to Germany. This comparison shall give a broader understanding for potential regulatory strategies and tools. On this basis, we will finally come to a conclusion on which further, or other instruments should be implemented in order to safeguard that microtargeting in political campaigning does not hamper but enhance the political process in our democratic civil society.

How micro-targeting works

Marketing has long been one of the most important functions in corporations to create sustainable success. Many of the principles and mechanisms can also be applied to politics and have already been used to understand political functions such as elections, referenda, governing, lobbying, and public service management.[1] Central to any marketing strategy in business and politics is the notion that any decision in an organization should be based on an in depth understanding of what the customer or voter needs and wants and how these needs are met by products and services. In a political context however, these products and services represent a complex set of offerings that relates to the candidate and political promises made during an election.[2] In order to understand microtargeting as a marketing tool in a political context, this section will first highlight the characteristics of commercial microtargeting. Second, the section will then transfer these characteristics to the political context and highlight essential differences.

Micro-targeting techniques used for advertising purposes

Since the 1950s marketing has evolved from a mass marketing approach to highly individualized, segmented marketing. With the rise of digital advertising technology and data analytics, the possibilities to segment and tailor messaging to fine-grained customer segments have become endless. Marketing strategies have ultimately become more customer-centric. While most interactions were initiated and controlled by the organization in classical mass marketing approaches, today interactions are multilateral and often initiated by the customer. Multi-channel communication strategies with tailored messages and seamless customer journeys across various touch points have become the new reality for marketers in all organizations. To fully enable these strategies, various data sources have to be connected and analyzed intelligently. In this context, microtargeting emerges as a means to execute these intelligent strategies.[3]

Microtargeting uses technological advances in all areas of marketing, such as database analytics, acquisition, customer relationship management, and relationship marketing.[4] They enable marketers to know who uses their products or services, why and how often they use them and what their main motivation is. It is said to provide new competitive tools, to increase retail power, and encourage partnerships between organizations.[5] Its effectiveness relies on the said intelligent interlinking of various data sources. Those data sources reflect the specific traits of particular customer segments. Big data and customer analytics allow marketers to

[1] See Bruce I. Newman, Reinforcing Lessons for Business from the Marketing Revolution in US Presidential Politics: A Strategic Triad. Psychology & Marketing, 33(10), 2016, pp. 781-795 and Wojciech Cwalina, Andrzej Falkowski, and Bruce I. Newman, Political marketing: Theoretical and strategic foundations. ME Sharpe 2011.

[2] See Wojciech Cwalina, Andrzej Falkowski, and Bruce I. Newman, Political marketing: The multidisciplinary approach. In William Benoit (Ed.), Praeger handbook of political campaigning in the United States, Santa Barbara, CA: Praeger Publications, 2016, pp. 101–119.

[3] See Björn Bloching and Andreas Heinz, Die Illusion der Kundenzentrierung- fünf unbequeme Thesen zum digitalen Marketing. Roland Berger Working Paper Series, 2016.

[4] See Bruce I. Newman, Reinforcing Lessons for Business from the Marketing Revolution in US Presidential Politics: A Strategic Triad. Psychology & Marketing, 33(10), 2016, pp. 781-795

[5] See Bruce I. Newman, Reinforcing Lessons for Business from the Marketing Revolution in US Presidential Politics: A Strategic Triad. Psychology & Marketing, 33(10), 2016, pp. 781-795, Cristina Ziliani and Silvia Bellini, From loyalty cards to micro-marketing strategies: Where is Europe's retail industry heading?, Journal of Targeting, Measurement and Analysis for Marketing 12.3, 2003, pp 281-289 and Adam Brandenburger and Barry J. Nalebuff, Co-opetition, Crown Business, 2011.

understand in detail where their customers are, what motivates them and what triggers their decisions.[6] In other words, it allows them to combine comprehensive individual and behavioral characteristics with transactional data such as purchasing histories.[7] Common data sources are internal datasets such as sales data, financial data, marketing data (e.g. campaign response data, website engagements, and loyalty programs), and service data. Additionally, many firms buy data from external sources to enrich their internal datasets. Today, geodemographic and lifestyle data add great value to define and target customer segments.[8]

Micro-targeting techniques used for political campaigning

Similar to commercial marketing campaigns, political campaigns also have the goal of reaching a particular segment with a specific message at the lowest possible cost.[9] In the context of political campaigns, classic consumer data (e.g. geodemographic - like estimated years of education, home ownership status, and mortgage information - and lifestyle data) is combined, at least in principle, with four specific kinds of voter data: Voter registration data, donor data, response data gathered through surveys and personal interviews, and campaign website data).[10] This allows campaign managers to affect voter preferences, fundraising behavior, and voting results instead of purchasing decisions.[11] For doing so, understanding the position of a voter in his social setting, their needs and wants, their personality, attitudes and motivations are essential for successful political microtargeting.[12]

While the analytical processing of this kind of data is widely the same, Newman carves out a number of characteristics that make political campaigns distinct from commercial campaigns. First, a political campaign needs to reach many voter segments with different interests but a shared expectation – that the candidate will hold his political promises after the election. In contrast, a customer will usually be quite well informed about the product or service characteristics before the purchase and thus not experience much uncertainty after buying it. Second, voter preferences are constantly changing and influenced by a very dynamic environment. While customer preferences are also changing in today's connected world, they do remain fairly constant on an aggregate level. Third, political campaigns are driven by many unforeseeable external events that may influence voter behavior significantly and require a candidate to quickly respond in an appropriate manner. In a commercial context, the impact of external events on customer preferences is much less frequent. Fourth, political campaigns usually have to deal with a lot of negative press coverage and find ways to respond accordingly to match the interests of various voter segments. Commercial campaigns seldom have to deal with negative press coverage at such a scale and can concentrate on a clear communication

[6] See Bruce I. Newman, Reinforcing Lessons for Business from the Marketing Revolution in US Presidential Politics: A Strategic Triad. Psychology & Marketing, 33(10), 2016, pp. 781-795

[7] Tianyi Jiang and Alexander Tuzhilin, Dynamic micro-targeting: fitness-based approach to predicting individual preferences, Knowledge and information systems 19.3, 2009, pp: 337.

[8] See Björn Bloching and Andreas Heinz, Die Illusion der Kundenzentrierung- fünf unbequeme Thesen zum digitalen Marketing. Roland Berger Working Paper Series, 2016.

[9] See David Nickerson and Todd Rogers, Political campaigns and big data, The Journal of Economic Perspectives 28.2, 2014, pp: 51-73.

[10] See David Nickerson and Todd Rogers, Political campaigns and big data, The Journal of Economic Perspectives 28.2, 2014, pp: 51-73.

[11] See David Nickerson and Todd Rogers, Political campaigns and big data, The Journal of Economic Perspectives 28.2, 2014, pp: 51-73.

[12] Aron O'cass and Rajan Nataraajan, At the polls: Continuing to explore voter psychology, Journal of Political Marketing 2.2, 2003, pp: 67-81.

which is less responsive. Last, political campaigns deal with an audience (i.e. voters), which is much more loyal to a certain party or candidate. This is due to the fact that political decisions are based on strong ideological values. Voters will thus seldom change their political decisions. Commercial campaigns on the other hand aim to build loyalty and cannot assume it a priori.[13]

Question on the differences with respect to its regulation

In light of these differences, the question therefore is which specific risks arise by the use of micro-targeting techniques for political campaigning, and whether or not this requires further or other regulations than its usage for commercial advertising purposes.

Theoretical-normative assessment

In order to answer the question of which specific risks arise by the use of micro-targeting techniques, it is necessary to delve deeper into the legal concept of protection that is concerned in both contexts of commercial advertising and political campaigning. Usually, the discussion refers, regarding both contexts, to privacy and/or data protection. However, only if it is clear against which specific risk privacy and/or data protection actually protects, it is possible to answer the question on the appropriate regulation addressing these risks. Indeed, discussions about the concept of privacy and/or data protection still consists of two essential unclarities: First, it is not yet comprehensively clear what the precise object(s) of protection actually is (or are); and second, which way is most appropriate providing, on the one hand, a data subject (e.g. a voter or consumer) for an effective and efficient protection and, on the other hand, not restraining the room of action of third parties (be it a commercial advertising actor or a political actor), disproportionately.[14] In particular, with respect to the new fundamental right to data protection under Art. 8 ECFR, there is an ongoing debate about the concept of protection of this right, and its relation to other fundamental rights, in particular, the right to private life under Art. 7 ECFR.[15]

Privacy and data protection

With respect to the use of micro-targeting techniques, at least, two aspects are clear. First, all concepts of privacy and/or data protection aim to protect individuals against an illegitimate intrusion into their private spheres.[16] The reasoning behind such a “right to be left alone” is the

[13] See Bruce I. Newman, Reinforcing Lessons for Business from the Marketing Revolution in US Presidential Politics: A Strategic Triad. Psychology & Marketing, 33(10), 2016, pp. 781-795

[14] See, with respect to the US American privacy discussion, instead of many others, Helen Nissenbaum, Privacy in Context, Stanford University Press 2010, pp. 67 et seq.

[15] See Paul de Hert and Serge Gutwirth, Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in: Erik Claes / Antony Duff / Serge Gutwirth (eds.), Privacy and the criminal law, Antwerp/Oxford: Intersentia, 2006, pp. 61–104; Antoinette Rouvroy and Yves Poullet: The Right to Informational Self- Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Serge Gutwirth / Yves Poullet / Paul de Hert / Cecile de Terwangne / Sjaak Nouwt (eds.), Reinventing Data Protection?, New York i.a.: Springer, 2009, pp. 45–76; Gloria, González-Fuster: The Emergence of Data Protection as a Fundamental Right of the EU, Cham i.a.: Springer, 2014; Maximilian v. Grafenstein and Wolfgang Schulz: The right to be forgotten in data protection law: a search for the concept of protection, in: International Journal for Public Law and Policy 5 (3) (2015), pp. 249–269.

[16] See, with respect to European law, ECtHR, Case of Halford vs. The United Kingdom from 25 June 1997 (application no. 20606/92), cip. 45; ECtHR, Case of Peck vs. the United Kingdom from 28 January 2003 (application no. 44647/98), cip. 61; ECtHR, Case of Copland vs. The United Kingdom from 3 April 2007 (application no. 62617/00), cip. 41; and with respect to US American privacy discussions, Helen Nissenbaum, Privacy in Context, Stanford University Press 2010, pp. 89 et seq.

idea that individuals would not be able to enroll their personality in a civil liberty society as autonomous, i.e. self-determined individuals if they were not able to pull back themselves into a certain private sphere.[17] This aim can be considered as the actual origin of all modern concepts of privacy and/or data protection.[18]

However, the idea of individual autonomy also leads to another aspect of protection, which is discussed, particularly, with respect to the German right to informational self-determination. Pursuant to this discussion, privacy and/or data protection do not only require an individual's right to be left alone but also that an individual can know what others know about him or her. The idea behind this thought is that individuals also need to know, at least to a certain extent, how they are perceived by others in order to be able to enroll as autonomous, self-conscious citizens. Rouvroy and Poullet stress, for example, that the right to privacy serves the "capacity for both reflexive autonomy allowing to resist social pressure to conform with dominant views and for deliberative abilities allowing participation in deliberative processes".[19] Similarly, Britz holds the unbiasedness of individual behavior as the essential guarantee provided for by the German right to informational self-determination. She calls this guarantee "internal freedom of development". This freedom guarantees, that the individual is able to reflect and distance him or herself from own and other's expectations on his or her behavior. On this basis, this guarantee makes also sure that the individual can influence the perception of others concerning him or herself in order to maintain and broaden his or her opportunities of social conduct.[20]

These specific guarantees are equally concerned by the use of micro-targeting techniques in both contexts. For example, an individual's specific guarantee to be left alone can be relevant if advertisers seek to send individuals, based on these techniques, advertising emails.[21] This guarantee can equally be concerned if political campaigners find out which voter is (still) indecisive and, therefore, tries to visit this individual at home. In both cases, indeed, this paper does not aim to answer the question of whether individuals shall have the specific right not to receive advertising emails or not being disturbed by a political campaigner knocking on their doors. Rather, it shall be stressed, so far, that this guarantee applies to the use of these techniques in both an advertising context, and the context of political campaigning. Comparably, the individual's specific guarantee to know, at least to a certain extent, what others know about him or her is also concerned in both contexts. Guaranteeing the unbiasedness of individual behavior, this guarantee seeks, in a commercial advertising context, to protect an individual against an illegitimate manipulation

[17] See, for instance, Gabriele Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaft- licher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Edmund Brandt / Martin Eifert / Bernd Holznagel i.a. (eds.), Offene Rechtswissenschaft, Tübingen: Mohr Siebeck 2010, pp. 588 to 591; Helen Nissenbaum, ibid., p. 81 quoting Stanley Benn (1971), Privacy, Freedom and Respect for Persons, in: Privacy, ed. J. R. Pennock and J. W. Chapman, New York: Atherton Press, pp. 1 to 27 (p. 24), reprinted in Philosophical Dimensions of Privacy: An Anthology, ed. F. Schoeman. Cam- bridge: Cambridge University Press, 1984, pp. 223– 244, as well as Jeffrey Reiman (1995), Driving to the Panopticum: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, Santa Clara Computer and High Technology Law Journal 11(1): pp. 27 to 44 (p. 33).

[18] See, for example, with respect to the German right to informational self-determination, Marion Albers, Informationelle Selbstbestimmung, Baden-Baden: Nomos 2005, pp. 211 and 212.

[19] See Antoinette Rouvroy and Yves Poullet: The Right to Informational Self- Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Serge Gutwirth / Yves Poullet / Paul de Hert / Cecile de Terwangne / Sjaak Nouwt (eds.), Reinventing Data Protection?, New York i.a.: Springer, 2009, p. 46.

[20] Gabriele Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaft- licher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Edmund Brandt / Martin Eifert / Bernd Holznagel i.a. (eds.), Offene Rechtswissenschaft, Tübingen: Mohr Siebeck 2010, pp. 571 to 574.

[21] See, for instance, Art. 13 of the ePrivacy Directive 2002/58/EU.

of their purchasing decision.[22] And in the context of political campaigning, this guarantee protects a voter against an illegitimate manipulation of his or her electoral decision. However, this point makes also clear that there are further, potentially, even more specific guarantees concerned, such as political participation rights.

Indeed, fundamental rights do not directly bind private parties, such as political parties and candidates,but they have an indirect effect on the private sector. The regulator has thus to balance, when establishing or interpreting ordinary law, the colliding fundamental rights of private parties. If the use of micro-targeting techniques leads to a potentially negative impact on such rights, the regulator hence has to take these rights into account in the course of its balancing exercise.[23] In fact, the use of micro-targeting techniques can actually not only be it in detriment of voters, but also conflict with the participation rights of competing political parties or candidates. This can be the case, for instance, if these parties or candidates do not have the same chances to get access to the necessary data or processing techniques. And this may lead to an essential difference in protection, compared to the use of micro-targeting techniques in a commercial advertising context.

Different specific objects of protection concerned

Focusing on voters, privacy and/or data protection could thus additionally aim, in the context of political campaigning, to protect an individual concerned against being manipulated in his or her process of decision against or for a political party or politician. Such a protection is typically provided for by the fundamental right to vote and stand as a candidate at elections to the European Parliament under Art. 39 ECFR. Art. 39 sect. 2 ECFR, states, at least, that the "Members of the European Parliament shall be elected by direct universal suffrage in a *free* and secret ballot" (underlining in *italic* by the author). Art. 40 ECFR refers, with respect to national elections, to national legislations of the Member States, which contain very similar, if not the same, conditions.[24] Thus, the use of micro-targeting techniques for political campaigning can also undermine, in principle, these political participation rights. If the use of micro-targeting techniques does not only concern the rights to private life under Art. 7 ECFR and/or to data protection under Art. 8 ECFR but also these (eventually even more specific) Citizen's Rights, these guarantees should be taken into account when deciding on which protection instruments may most *effectively* protect the voters.

Indeed, as stressed previously, the relation between the new right to data protection with further fundamental rights is not yet clear. In particular, it is unclear whether the concept of data protection refers also to those guarantees provided for by the other fundamental rights. Many authors however consider that the ultimate aim of the fundamental rights to private life under Art. 7 ECFR and/or data protection under Art. 8 ECFR, respectively, is (also) to protect

[22] Cf. the requirements regarding advertising in audiovisual media under Art. 9 sect. 1 lit. a) and b) of the Audiovisual Media Directive 2010/13/EU.

[23] See Liv Jaeckel, Schutzpflichten im deutschen und europäischen Recht – Eine Untersuchung der deutschen Grundrechte, der Menschenrechte und Grundfreiheiten der EMRK sowie der Grundrechte und Grundfreiheiten der Europäischen Gemeinschaft, Baden-Baden: Nomos, 2001, p. 103, who stresses the many commonalities of all three fundamental rights regimes, i.e. the ECHR, the ECFR, and the German Basic Rights regarding the state duty of protection; Rolf Eckhoff: Der Grundrechtseingriff, Köln i.a.: Carl Heymanns, 1992, regarding the terminology, pp. 288 to 290.

[24] See, for instance, Art. 38 sect. 1 GG (i.e. of the German Basic Law).

(at least indirectly) the exercise of those further fundamental rights.[25] And also the European Court of Justice refers, more and more, to further fundamental rights when elaborating on the concepts of the fundamental rights to private life and data protection under Art. 7 and 8 ECFR.[26]

Building upon this approach, in principle, not only individual fundamental rights come into question in order to assess whether a certain action conflicts with the concept of privacy and/or data protection, but even abstract constitutional principles.[27] Indeed, such abstract principles cannot justify, per se, a restriction of the campaigners scope of action. But such a principle concerned can give more weight to individuals' fundamental rights in the course of the regulators' balancing exercise.[28] In any case, n the context of political campaigning, such a principle concerned could be the principle of democracy. The reasoning behind this thought is that the use of micro-targeting techniques for political campaigning could be considered as conflicting with the proper functioning of democratic elections. On the one hand, as discussed before, the use of these techniques could result in an illegitimate manipulation of a voter's decision. However, on the other hand, and this was not yet stressed, so far, exhaustively, the usage of these techniques may also enhance the individual's decision making process because it helps voters coming to a decision that fits best to his or her political opinion. In this case, the use of micro-targeting techniques for political campaigning could also enhance electoral processes. Indeed, whether the one or the other result is more valuable depends on how democracy is theoretically conceptualized.

Risk assessment regarding the concept of democracy

In order to answer the question of whether the use of micro-targeting techniques for political campaigning rather creates a risk against democracy than enhances the voters' political decision-making process, the subsequent paragraphs will examine: first, how democracy is (or can) theoretically (be) conceptualised; second, which specific risks against democracy are essentially discussed, in literature; and third, whether the factual differences between the use of micro-targeting techniques in a commercial advertising context and the context of political campaigning requires a re-calibration of this risk assessment.

---

[25] See Marion Albers, Realizing the Complexity of Data Protection, in: Serge Gutwirth/Paul de Hert/Ronald Leenes (Eds.), Reloading Data Protection, Dordrecht/Heidelberg/London/New York: Springer, 2014, S. 213 – 235; Maximilian v. Grafenstein and Wolfgang Schulz: The right to be forgotten in data protection law: a search for the concept of protection, in: International Journal for Public Law and Policy 5 (3) (2015), pp. 249–269; cp. also Paul de Hert and Serge Gutwirth, Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in: Erik Claes / Antony Duff / Serge Gutwirth (eds.), Privacy and the criminal law, Antwerp/Oxford: Intersentia, 2006, p. 44; Antoinette Rouvroy and Yves Poullet: The Right to Informational Self- Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Serge Gutwirth / Yves Poullet / Paul de Hert / Cecile de Terwangne / Sjaak Nouwt (eds.), Reinventing Data Protection?, New York i.a.: Springer, 2009, pp. 61 and 70.

[26] See ECJ C-465/00, C-138/01 and C-139/01 (Rechnungshof vs. ORF), cip. 89, taking, implicitly, the freedom to choose an occupation and the right to engage in work under Art. 15 ECFR into account; ECJ C-293/12 and C-594/12 (Digital Rights vs. Ireland), cip. 37, referring to Opinion of Advocate General Cruz Villalón delivered on 12 December 2013 on Case C-293/12, cip. 52, regarding the freedom of expression under Art. 11; ECJ C-362/14 (Schrems vs. Facebook), cip. 39, with respect to the fundamental right to effective judicial protection under Art. 47 ECFR.

[27] Cf. David Wright, Michael Friedewald, and Raphaël Gellert, Developing and testing a surveillance impact assessment methodology, in: International Data Privacy Law 5 (1) (2015), pp. 40–53 (40).

[28] Cf. Dietlein, Johannes: Die Lehre von den grundrechtlichen Schutzpflichten, Berlin: Duncker & Humblot, 2005, pp. 104 and 105.

Democratic representation as an interactive process

The term “democratic representation” means that political decisions are not directly made by the citizens of a democratic state, but only indirectly. In doing so, the citizens vote, by means of a universal, free and secret ballot, the parliament representing the “voters’ political will”. However, while the notion of a “voters’ political will” seems to imply a static, already existing entity that just has to be catched up by politicians, a current trend amongst political scientists favors a more dynamic-interactive model. Pursuant to this model, democratic representation can rather be explained as a dynamic and interactive communication process between the voters as representees and the political delegates as representatives. Such a process does not follow a one-directional flow of information, i.e. of political opinions, from the voters to the delegates. Instead, it is the interactive process that creates itself the “aggregated” political opinions of the voting population. In this process, electoral campaigns can be understood as a specific mode.[29] Building upon this concept, it is Hoffmann who carves out which function micro-targeting techniques can have in such an interactive process shaping and aggregating public opinions and policies.

In Hoffmann’s opinion, micro-targeting in the context of political campaigning does not only constitute an effective and efficient means for political campaigning. Rather, the usage of micro-targeting techniques “influences the perception itself that political parties get about voters and citizens, and this perception, in turn, influences how citizens perceive themselves in the political process.”[30] Hoffmann draws from this function of micro-targeting techniques in the process of political campaigning two, so far, preliminary conclusions: On the one hand, the use of micro-targeting techniques can enhance the communication process between voters and delegates, or more precisely, candidates (this means, between representees and representatives). Political candidates are able to arrange political arguments that personally address the voter’s needs, mobilize the voters to participate in the political process, help them orient themselves within the political landscape and identify with one of the candidates. On the other hand, she stresses, the relationship between voters and candidates is highly asymmetric. Voters do neither control which information political campaigners aggregate about them, nor do they have a similar power of information about, or rather, over “their” candidates. While campaigners can hence influence the decision process of voters, voters are much less able to control the behavior of the candidates. In addition, these informational power asymmetries are the more increasing the more the use of micro-targeting techniques becomes institutionalized. However, in Hoffmann’s opinion, it is yet too early in order to come to a final conclusion on whether or not the use of micro-targeting really leads to a loss of representative democracy.[31]

---

[29] See Jeanette Hoffmann (forth.), Big Data im Wahlkampf: Wählermodus, Micro-Targeting und Repräsentationsansprüche, “Dimensionen von Big Data: eine politikwissenschaftliche Systematisierung”, in: Heil, Reinhard; Kolany-Raiser, Barbara; Orwat, Carsten: „Big Data und Gesellschaft. Eine multidisziplinäre Annäherung“, Springer, pp. 13 and 14, referring to Pitkin, H. F. (1967). The concept of representation. Berkeley and Los Angeles: University of California Press, p. 8; Saward, M. (2006). The representative claim. *Contemporary Political Theory 5*: 297-318, pp. 303, 304 and 310; as well as Rosanvallon, P. (2006). *Democracy past and future*. New York: Columbia University Press, p. 78.

[30] See Jeanette Hoffmann (forth.), Big Data im Wahlkampf: Wählermodus, Micro-Targeting und Repräsentationsansprüche, “Dimensionen von Big Data: eine politikwissenschaftliche Systematisierung”, in: Heil, Reinhard; Kolany-Raiser, Barbara; Orwat, Carsten: „Big Data und Gesellschaft. Eine multidisziplinäre Annäherung“, Springer, p. 13: “(Big Data) beeinflusst vielmehr das Bild, das Parteien sich von Wählern und Bürgern machen und dieses Bild wirkt wiederum darauf ein, wie BürgerInnen sich selbst im politischen Prozess verstehen.”

[31] See Jeanette Hoffmann (forth.), Big Data im Wahlkampf: Wählermodus, Micro-Targeting und Repräsentationsansprüche, “Dimensionen von Big Data: eine politikwissenschaftliche Systematisierung”, in: Heil, Reinhard; Kolany-Raiser, Barbara; Orwat, Carsten: „Big Data und Gesellschaft. Eine multidisziplinäre Annäherung“, Springer, pp. 16 to 18.

Specific risks caused by political micro-targeting

At this point, it is important to recognize (and very likely true) that much research still has to be done in order to be able to definitely say whether or not the use of micro-targeting techniques for political campaigning leads to a loss of representative democracy. However, such a concrete loss is not necessary, actually, for a regulation that does not address concrete losses but rather risks. This is, at least, the case with respect to privacy and data protection laws, which follow a risk regulatory approach.[32] The application of such a risk regulatory regime does not wait until a real loss has already occurred. Instead, such a regime provides for protection instruments in order to prevent a situation that would turn, without such instruments, into a real damage for a specific object of protection.[33] From this perspective, it is hence necessary to determine, more specifically, the possible risks that can lead to a negative impact on a representative democracy.

The previous analysis has already shown that such risks can be, so far, an illegitimate manipulation of the decision process of a voter.[34] However, there are also further risks discussed in legal literature. With respect to the use of micro-targeting techniques for political campaigns in the US, for instance, Rubinstein sums up the discussion on (what he calls) "political harms" pursuant to three categories: The first category refers to the harm of "political inequality". This harm may occur if political campaigners address certain voter groups that are, pursuant to the voter models constructed on the basis of the micro-targeting techniques, preferable from the perspective of the political campaigners. This can lead to the result that other groups of voters get completely marginalized. This risk can lead to a negative impact on the principle of representative democracy since this principle requires that all voters should be represented, and not only that types of voters being captured by the models.[35]

The second category refers to a harm that the authors of this paper call "political opportunism". In this case, political candidates do not advocate a certain political opinion because "they are necessarily the most important issues" but "because they help create a strategic advantage".[36] Indeed, this actually is not a new harm only caused by the use of micro-targeting techniques. However, Rubinstein stresses that this opportunistic attitude gets

---

[32] See Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey: Editorial – Risk management in data protection, in: International Data Privacy Law 5 (2) (2015), pp. 95–98; Costa, Privacy and the precautionary principle; Raphaël Gellert, Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative, in: International Data Privacy Law 5 (1) (2015), pp. 3–19; with particular respect to the Data Protection Directive 95/46/EC, the Article 29 Data Protection Working Party (set up under Article 29 of Directive 95/46/EC): Statement on the role of a risk-based approach in data protection legal frameworks, 30 May 2014, 14/EN, WP 218, URL: http://ec.europa.eu/justice/data-protection/article- 29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, p. 2; as well as the OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data in Article 2.

[33] See, with a general view on legal risk regulation, Liv Jaeckel, Gefahrenabwehrrecht und Risikodogmatik – Moderne Technologien im Spiegel des Verwaltungsrechts, Tübingen, Mohr Siebeck 2010, pp. 49 et seq.; with particular respect to privacy laws, already at Arthur R. Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, in: Michigan Law Review 67 (6) (1969), pp. 1089–1246 (1221).

[34] See above under point "Privacy and data protection"; indeed, another risk even refers to negative impacts on the scope of autonomous action of the delegates themselves, see above under point "Democratic representation as an interactive process".

[35] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 33, referring to D. SUNSHINE HILYGUS & TODD G. SHIELDS, THE PERSUADABLE VOTER: WEDGE ISSUES IN PRESIDENTIAL CAMPAIGNS 155 (2008); KATE KENSKI, BRICE W. HARDY & KATHLEEN HALL JAMIESON, THE OBAMA VICTORY: HOW MEDIA, MONEY AND MESSAGE SHAPED THE 2008 ELECTION 304-06 (2010), pp. 4, 151, and 186 to 193.

[36] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 33, quoting D. SUNSHINE HILYGUS & TODD G. SHIELDS, THE PERSUADABLE VOTER: WEDGE ISSUES IN PRESIDENTIAL CAMPAIGNS 155 (2008); KATE KENSKI, BRICE W. HARDY & KATHLEEN HALL JAMIESON, THE OBAMA VICTORY: HOW MEDIA, MONEY AND MESSAGE SHAPED THE 2008 ELECTION 304-06 (2010), p. 187.

supported, significantly, by micro-targeting techniques because these techniques make politicians even more "distorted and insular". In his opinion, "(D)distortion occurs when candidates precisely calibrate which message will appeal to certain individuals, create multiple versions of the same message, and deliver them to individuals meeting the predetermined criteria, via email, online ads, cable TV, or social media.[37] In contrast, the term "insularity" sums up, as a side effect of "distortion", the observation that political leaders are, more and more, less likely to "lead" because they are more tempted "to reinforce latent opinions than to reframe them."[38]

Finally, the third category refers to the situation where the gap between campaigning and governing increases because the increasing personalization, or in this context rather, singularization of political promises given during the campaigning process hinders the evolvement of a general public discourse. The consideration behind this concern is that the smaller a public discourse gets, the weaker the public pressure is that enforces a candidate to hold his or her promise when he or she has become a delegate.[39] This potential harm builds thus upon the preceding considerations that a political campaigner gets, more and more "distorted and insular". Both risks correspond to the considerations made by Hoffmann that voters are much less able to control the behavior of the candidates than campaigners are able to influence the voters' electoral decision making process.[40]

Taking the factual differences of both contexts into account

On this basis, it is now possible to examine whether, and if so, in which way the factual differences between the use of micro-targeting techniques in a commercial advertising context and the context of political campaigning, require to re-calibrate the previous risk assessment. In doing so, the subsequent analysis will illustrate that all differences actually increase the risks previously described.

All risk increasing factors have in common to result from the higher knowledge uncertainty under which both voters and candidates are able to act. On the one hand, the uncertainties that a campaigner has to face lead to an increase of risks as: First, voter preferences are said to be much more fluent than the preferences of a commercial customer; second, in contrast to commercial campaigns, political campaigns are influenced by more unexpected external events to which a candidate has to react in order to catch up with a voter's opinion on that event; and third, the pressure of negative publicity is higher on political candidates

---

[37] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 33, referring to David Parry, Big Data: What Happens When Elections Become Social Engineering Competitions, PERSONAL DEMOCRACY MEDIA (June 26 2012), http://techpresident.com/news/22466/op-ed-big-data-what-happens-when-elections-become-social-engineering-competitions; as well as Tim Murphy, Inside the Obama Campaign's Hard Drive, MOTHER JONES (Sept./Oct. 2012), http://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting?page=2 (noting that a single Obama fundraising email came in no less than 11 different varieties and that Romney's campaign boasted that: "Two people in the same house could get different messages. ... Not only will the message change, the type of content will change").

[38] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 33, quoting W. Lance Bennett and Iarol B. Manheim, The One-Step Flow of Communication, 608 ANNALS AM. ACAD. POL. & SOC. SCI. 213, 215-16 (2006), p. 213.

[39] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 33, referring to D. SUNSHINE HILYGUS & TODD G. SHIELDS, THE PERSUADABLE VOTER: WEDGE ISSUES IN PRESIDENTIAL CAMPAIGNS 155 (2008); KATE KENSKI, BRICE W. HARDY & KATHLEEN HALL JAMIESON, THE OBAMA VICTORY: HOW MEDIA, MONEY AND MESSAGE SHAPED THE 2008 ELECTION 304-06 (2010), p. 189, as well as Jon Gertner, The Very, Very Personal Is the Political, NY TIMES (Feb. 15, 2004), http://www.nytimes.com/2004/02/15/magazine/15VOTERS.html.

[40] See above under point "Democratic representation as an interactive process"; indeed, another risk even refers to negative impacts on the scope of autonomous action of the delegates themselves.

than on commercial entities, what makes it more difficult for political to react appropriately. All three factual uncertainties increase the risk that a political campaigner tends to become "distorted and insular". The ability to flexibly address the personal preferences of a single voter in a bilateral, i.e. non-public way, opens a floodgate for opportunistic communication strategies.

On the other hand, as pointed out several times before, voters are less able to to control whether or not a political candidate keeps, once elected as a delegate, his or her promises given during the campaign. In contrast, in a commercial advertising context, a customer usually experiences much less uncertainty about the product or service quality after he or she has bought the product. This risk of such a loss of control is further increased by the fact that voters are, in light of their ideological bindings to a political orientation, more loyal in the political context and, therefore, less likely to get rid of a certain candidate.

So far, the losses potentially caused by the use of micro-targeting techniques in the context of political campaigning appears, hence, to be higher and/or more than its potential gains expected in the form of more mobilized voters groups. However, this result does not necessarily mean that the use of micro-targeting techniques for political campaigning should be forbidden overall. Rather, the question is of whether, or more precisely, how these risks might be mitigated to an extent being lower than the potential gains for a representative democracy.

Current regulations in the US and the EU/Germany

In order to answer the question on which regulatory strategies and tools might come into question in order to mitigate these risks, it is useful to examine how these risks are addressed currently. In this regard, it is particularly worth to examine the situation in both the US and the EU. The reason for this is that such a comparison broadens the understanding on the effectiveness and efficiency of different tools and strategies.

US legislation

Coming from a European background, the most significant observation is that the usage of the different categories of data, as mentioned previously, is widely unregulated under US law.

Almost no regulation for types of data used for political campaigning

With respect to voter registration data (VRD), state election laws rather favor, pursuant to the legal assessment by Rubinstein, the public disclosure of personal data from voter rolls, instead of restricting, or at least, controlling it.[41] This data does not only contain information about name, address, signature, phone number, gender, and party affiliations of a voter. Typically, VRD also includes voter history, that is, where, when, and how often someone

[41] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 13.

votes.[42] Only the social security numbers are redacted from the publication, as well as certain information regarding vulnerable individuals.[43]

Response data is also not regulated, just like campaign website data is widely unregulated.[44] In particular, campaign website data has become a central source of information for any political campaign. Required data includes any registration data collected during sign-up processes on the websites. Volunteered data refers to descriptive data voters give to the campaigns through interactions online as well as observations of their interactions on blogs and social media sites. Observed data refers to data gathered during online interactions, for example through IP addresses, website interactions, or cookies.[45]

Only donor data falls under a rather strict legal regime, except for privacy purposes. In light of the absence of a direct regulation, there is only a limited control of the usage of that data for political micro-targeting campaigns. This limited control consists in a slight form of self-regulation.[46]

Possible protection instruments

In light of the widely unregulated data processing landscape, it might be worth to examine which protection instruments are discussed in US literature. However, from a European perspective, there are barely new ideas. Amongst them, disclosure duties obliging a political campaigner to inform the voter concerned about the use of micro-targeting techniques appears to be the most prominent one. Such duties go hand in hand with the expectation that voters would not only be able to control the disclosure of information about them, but could also be used, through the public discourse, to put campaigners under pressure in order to adhere to certain processing principles such as of data quality. Indeed, the US discussion recognizes well that voters concerned might not use their possibility to make an "informed choice" about the disclosure of information. Therefore, also a direct, cross-sectoral regulation is discussed, just like the recently amended COPPA rule, which provides for further rights, such as to access, rectify and delete certain information.[47]

Little chances for further regulation

However, Rubinstein comes, in this regard, to the conclusion: "obviously, voter privacy is at best a secondary or tertiary issue compared to war and peace, the economy, health care and retirement benefits, and so on. So it is quite possible that voter privacy issue will not garner sufficient attention to provoke these salutary changes in campaign data practices."[48]

[42] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, pp. 5 to 7.
[43] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 13.
[44] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 13.
[45] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 5-18.
[46] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 13.
[47] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 36 to 39.
[48] See Ira Rubinstein, Voter Privacy in the Age of Big Data, URL: http://ssrn.com/abstract=2447956, p. 40.

EU legislation

In contrast to the US regulatory situation, it can be said that the use of micro-targeting for political campaigning is, in the EU, heavily regulated.

Cross-sectoral approach of data protection law

The European General Data Protection Regulation (GDPR), which comes into force the 28th May 2018, applies a cross-sectoral approach covering not only data that relates to identified individuals but even to individuals who are just identifiable.[49] The automated processing of personal data is only allowed if it is based on the consent of the individual concerned or another legitimate basis laid down by law.[50] Pursuant to this law, the data previously described has to be considered as personal data because micro-targeting for political campaigning seeks to identify a single voter, by singling him out from the group of citizens entitled to vote.[51] Since the GDPR is applicable to all types of data, so long as it is personal data, the processing of this data for political campaigning purposes must be based either on a legitimate basis provided for by law, or on the individual's consent.[52] Furthermore, the controller of the data processing (which is, most probably, the campaigner because it sets, at least, the purposes of the processing)[53] has to apply several rights and duties in favour of the voters, which are, compared to the US discussion, rather extensive.[54]

Legitimate basis required, and further rights and duties

Since the processing of that kind of data usually starts before a voter can consent to it, the campaigner has to base the data processing on another legitimate basis laid by law.[55] So long as the use of micro-targeting techniques for political campaigning is not regulated by national provisions, the controller has to base the processing on the general clause of its legitimate interests under Art. 6 sect. 1 lit. f) GDPR.[56] The use of micro-targeting techniques for political campaigning could only be based on this provision so long as the legitimate interests of the campaigner are not overridden by the interests of the voters. Indeed, when carrying out this balancing exercise, not only the campaigners interests must be taken into account, but also the interest of the public in an enhancement of electoral opinion-making process by the use of micro-targeting techniques should be taken into account.[57] However,

[49] See Art. 2 sect. 1 in combination with Art. 4 lit. a) GDPR (EU) 2016/679; see the same approach already already implemented through Art. 3 sect. 1 in combination with Art. 2 lit. a) Data Protection Directive 95/46/EC.

[50] See Art. 5 sect. 1 GDPR (EU) 2016/679; see, here again, the same approach already already implemented through Art. 3 sect. 1 in combination with Art. 7 Data Protection Directive 95/46/EC.

[51] See recital 26 sent. 2 GDPR (EU) 2016/679.

[52] See Art. 6 sect. 1 GDPR.

[53] See Art. 4 no. 7 GDPR.

[54] See, in particular, Art. 12 to 22 GDPR.

[55] The political campaigner usually sets the purpose of the data processing and is, consequently, the data controller, pursuant to Art. 4 lit. 7 GDPR (EU) 2016/679.

[56] Pursuant to Art. 6 sect. 1 lit. e) GDPR (EU) 2016/679, the processing could also be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; this might be the case (even if this is rather doubtful) if a national legislator comes to the conclusion that the enhancement of voters' participation in the political process is in the public interest and delegates the use of microtargeting to a certain entity.

[57] Cf. the Art. 29 Data Protection Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, 844/14/EN, WP 217, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, pp. 28 and 29.

in light of the specific risks described, the “legitimate interests” clause will nevertheless be applicable only if additional safeguards mitigate these risks.[58]

Supposed, these safeguards would be met, the controller has to meet several rights and duties, such as the voter’s right to access the data, correct and complement the data, delete and/or restrict the data, transfer the data to another controller like another political party or candidate, and object the data processing.[59] The campaigner has also to inform the voter, in particular, about the types of data used, sources from which the data stem, and the purpose of the processing.[60] With respect to the profiling of individuals, which is applicable to political micro-targeting, there are particular information duties. These require the political campaigner to inform the voter about “the existence of automated decision-making, including profiling, (...) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject”.[61] This means that the campaigner has to inform the voter about the specific risks previously described.

Processing principles, in particular, purpose limitation

Furthermore, the campaigner has to meet must meet the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality.[62] In particular, the principle of purpose limitation requires that the processing of data, which was collected for other purposes than political campaigning, must not be incompatible with the campaigning purposes.[63] This requires the campaigner to conduct an assessment by taking several criteria into account, such as: the nature of the data, the context in which the data was collected, the reasonable expectations of the individual, and the potential impact on the individual. In this regard, here again, additional safeguards are to be taken into account that mitigate the potential impact on the voter.[64]

Interims conclusion:

In conclusion, while the use of micro-targeting techniques for political campaigning is widely unregulated under US law, in the EU, its use is allowed only if the campaigner implements additional safeguards that mitigate the specific risks previously described. This is necessary, in particular, in order to to avoid: first, that the interests of the voters override the campaigners interests in the data processing (Art. 6 sect. 1 lit. f GDPR); and second, that the

---

[58] Cf. the Art. 29 Data Protection Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, 844/14/EN, WP 217, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, pp. 33 et seq.

[59] See Art. 15 to 21 GDPR.

[60] See Art. 13 and 14 GDPR, respectively.

[61] See Art. 13 sect. 2 lit. f) or Art. 14 sect. 2 lit g) GDPR, respectively.

[62] See Art. 5 sect. 1 GDPR.

[63] See Art. 5 sect. 1 lit. b) GDPR.

[64] See Art. 29 Data Protection Working Party, Opinion 03/0213 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, pp. 23 et seq.

processing of data, that was not originally collected for political campaigning purposes, is not incompatible with these purposes (Art. 5 sect. 1 lit. b) GDPR).

Conclusion: “Safeguards” in order to push the use of micro-targeting techniques for political campaigning into a sustainable direction

This leads us to the concluding question on how to mitigate the specific risks caused by the use of micro-targeting techniques for political campaigning. First of all, the specific risk that the use of these techniques illegitimately manipulates the voter’s decision-making process can be addressed by informing the individual. This risk-mitigation strategy is well seen with respect to the US situation, as well as appropriately addressed by European data protection law. In particular, the information duties applicable to profiling can mitigate this risk since they require the campaigner to inform the voter, amongst others, about the potential impact on him or her. Thus, the information must be suitable in order to avoid that the voter does not autonomously give his or her vote because he or she is manipulated by the usage of the micro-targeting techniques.

More complex is an answer to the question of how to mitigate the other specific risks as previously described. The use of micro-targeting techniques can lead to a negative impact on a representative democracy because candidates are tempted to become, more and more, opportunistic. This can be the case because candidates specifically address what single voters want to hear, in a purely personal (i.e. non-public) way. The public can hence not question anymore these promises, nor whether the candidate keeps the promises, after he or she has been elected. This is particularly relevant since certain factual circumstances in the context of political campaigning further increase these risks. For instance, political campaigners act under higher knowledge uncertainties than private companies in a commercial advertising context, what puts them further under pressure when trying to achieve their electoral aims.

Indeed, one may ask whether such abstract constitutional principles are legally relevant at all: First, some readers might consider that concepts of privacy and/or data protection do actually not address risks against further fundamental rights or abstract constitutional principles; second, fundamental rights do not directly bind private parties, such as political campaigners, but only the State; and third, this might be even more the case with respect to abstract constitutional principles. However, in our opinion, the concept of data protection should be constructed in a way aiming to protect also other (eventually more specific) fundamental rights and even abstract constitutional principles. Such an approach makes it possible to determine, precisely, the actual specific risks and, as a consequence, the instruments protecting against these risks effectively. Furthermore, even if fundamental rights do not directly bind private parties, the regulator has to balance the colliding fundamental rights when establishing or interpreting ordinary law. This means, the rights of political campaigners using micro-targeting techniques must be weighed against the rights of voters concerned by these techniques (as well as competing parties and/or candidates who may not get fair access, for instance, to the techniques and/or necessary data). And in the

moment such fundamental political participation rights are specifically concerned, a potentially negative impact on the principle of democracy can give further weight to these individuals' fundamental rights concerned.

Thus, in order to mitigate the risks overall, it is necessary to not only assess the risks against individuals' rights concerned but also against the concept of representative democracy. Since this is an abstract principle, it is reasonable to address these risks not by instruments protecting specific individuals, but on a societal-structural level. Such structural protection instruments can be, for instance, mechanisms that safeguard that all parties get fair access to the necessary data and/or analytical instruments, under the condition that this does not conflict with the voters' rights, of course. Indeed, this simultaneously protects also the competing parties' and/or candidates' political participation rights. The same is actually the case, with respect to the voters' information rights. These information rights do not only protect the voters but also safeguard, on a societal level, that specific uses of micro-targeting techniques can be monitored and questioned in the public. This is well seen, for instance, with respect to the situation in the US. However, there are also further protection instruments that function on a societal-structural level, only. For example, independent authorities, such as data protection authorities, could use their monitoring rights (or should be entitled), specifically, in order to systematically monitor how political campaigners use micro-targeting techniques. If these authorities come to the conclusion that certain practices lead to risks being disproportionate in relation to the gains for the political process overall, they could and should restrict such practices. Such a regulatory strategy implies, indeed, as Hoffmann pointed out, further research to be conducted. In particular, such research projects should be interdisciplinary carried out by various research partners, including classic and new media companies. There are two reason for this: First, new media companies can survey very well how their platforms are used by political campaigners in order to deliver certain messages to single voters, bilaterally; second, classic media companies can help push certain messages into a public debate. However, the fact that such research has to be conducted does not mean that there is no regulation needed, in advance. Rather, the risk regulatory approach just makes it possible to react, in time, with such research projects to questionable developments.

Last but not least, in light of the specific risks caused by the use of micro-targeting techniques, the European cross-sectoral approach appears to be preferable to the regulatory approach applied in the US. At least, having Rubinstein's concern in mind, the US approach may indeed lead to the situation that appropriate protection gets forgotten in the public discourse focusing on "more important" needs of a society. On the other hand, also the European approach has disadvantages. The first disadvantage is that the cross-sectoral approach inevitably leads to legal uncertainty. In the moment the processing of all kinds of personal data falls under the regulation, campaigners likely tend to be reluctant to use micro-targeting techniques even if they would like to use it in a way that sufficiently mitigates its risks. This leads to the second disadvantage because such a comprehensive regulation can quickly lead to over-regulation. The amount of rights and duties established in the law (i.e. the GDPR) is massive. Complying with all these requirements makes it difficult, in particular in light of the legal uncertainty described, for political campaigners, which operate with much less resources than companies in the commercial advertising context do. However, in the very end, if data protection authorities wisely use their competences, then they can fully play on the comparative advantage of the European approach by reacting, fast and accurately, to

questionable uses of micro-targeting techniques, pushing this new polito-technological development into a sustainable direction. In this case, micro-targeting techniques for political campaigning can indeed be a significant factor for the enhancement of electoral decision-making processes in a democratic civil liberty society.