

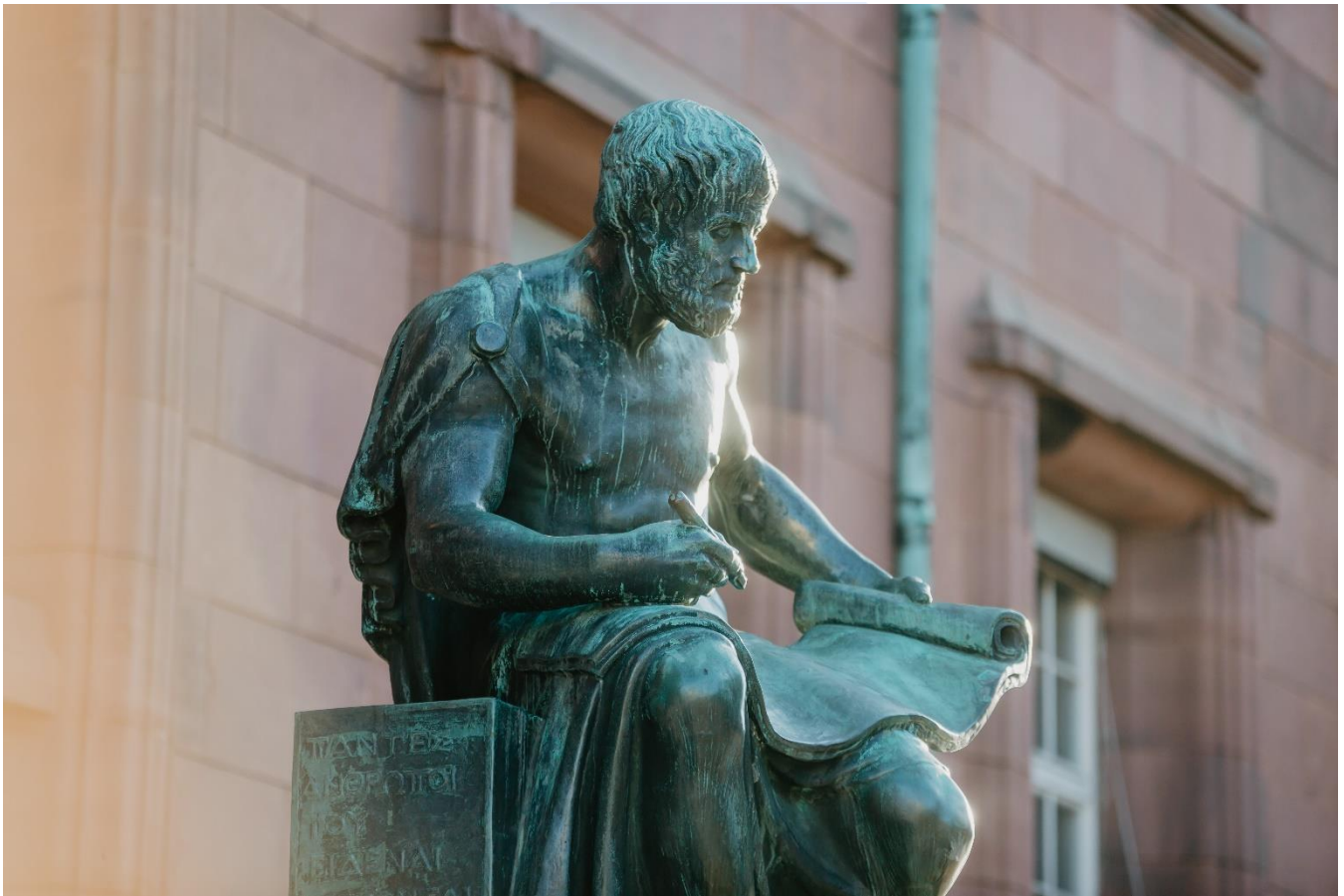
# Geopolitics of Tech

New Technologies, New Empires, New Strategies?

Syllabus

Amélie Hennemann-Heldt / Moritz Hennemann

January 2025



© Sandra Meyndt

## **Abstract**

This Syllabus supplies cases, texts, and materials to 20 sessions of a Course in Global Digital Policy. The Syllabus combines authoritative contributions in the field with introductory literature in order to foster a holistic learning experience. Departing from the key technological and economic underpinnings of today's Information and Algorithmic Society, the Course covers diverse areas of digital policy, both from a topical and a geopolitical viewpoint: from the Internet's first rules' genealogy to landmark regulations such as the GDPR, from Silicon Valley to Brussels and to Beijing.

## **Keywords**

Digital Law, Data Law, AI Law, Digital Regulation, Digital Policy, AI Policy, Global Tech Governance, Global Digital Law, Global Data Law, Global Digital Regulation, Digital Strategies, Data Strategies

## **Disclaimer**

External links make – for purely academic purposes – reference to third-party content. The authors or their respective institutions bear no responsibility for the content, the accuracy or the legality of the external sites / sources / any subsequent link. When linking no infringing content was observed or is known to us. If we are notified of any infringement in the future, we will immediately act and remove the link respectively.

# Introduction

The Information Society of the 21st century is rapidly evolving. Not only issues of an open, free, and digital communication connecting the world through the Internet are at stake. There is a fierce competition along the different layers of digital technologies (infrastructure, platforms, content, rules). The U.S., China, and Europe are each pursuing their own approach in this endeavour. Are we dealing with “digital empires” (Bradford) that are imposing (and exporting) their respective “model” of a digital society? The Chinese “Digital Silk Road” project, for example, is certainly not just about digital infrastructure. Conversely, U.S.-American so-called Big Tech companies act as “ambassadors” for the “American way”, promoting their business models worldwide. The European Union, in turn, is setting globally recognised legal standards (such as the GDPR). The outcome of this competition seems open, until now. At the same time, the rest of the world is often overlooked in this conversation, although most users of digital technologies do not come from the abovementioned countries. How are infrastructure, platforms, content, and rules developing outside these “digital empires”? What dependencies and interdependencies play a role? What partnerships should be sought?

Against this backdrop, this Course is dedicated to global digitalization, the associated regulatory approaches, the geopolitical contexts, and, above all, the (recurring) social conflicts of interest in dealing with new technologies.

This Syllabus supplies cases, texts, and materials to 20 sessions of a Course in Global Digital Policy. The Syllabus encompasses official documents issued by government institutions, essential (academic) writings on the respective subject, journalistic pieces, and (suggested and more extensive) further reading. The Course was part of a Summer School organized by the German Academic Scholarship Foundation (Studienstiftung des Deutschen Volkes) that was held at St Edmund Hall, University of Oxford in August 2024.

The goal of this Syllabus is to combine authoritative contributions in the field with introductory literature in order to foster a holistic learning experience. Departing from the key technological

and economic underpinnings of today's Information and Algorithmic Society, the Course covers diverse areas – from law to policy, from topical to geopolitical viewpoints, from the Internet's first rules' genealogy over landmark regulations such as the GDPR, to AI governance, from Silicon Valley to Brussels and Beijing. We aimed at taking a closer look at the existing and emerging (legal and governance) frameworks, their influence on other policy areas, and engaging with arising challenges of newer technologies such as generative AI.

As any list, this Syllabus is highly selective and, in that way, limited. We tried to mitigate our biases, but there is no way to deny that our setting in Europe and Germany – as well as our very own research – has in many ways shaped our selection. We therefore do not and cannot claim that the selection is balanced.

Things are moving fast in this area and most actors are eager to leave a mark. What is considered disruptive today might be outdated tomorrow. Nevertheless, certain fundamental questions arise again and again. Consequently, this Syllabus is only a starting point. We warmly welcome recommendations for the list in order to close gaps and to develop the list with us! Please drop us an e-mail to [a.heldt.ext@leibniz-hbi.de](mailto:a.heldt.ext@leibniz-hbi.de) and [moritz.hennemann@jura.uni-freiburg.de](mailto:moritz.hennemann@jura.uni-freiburg.de).

Sincerely yours,  
Amélie Hennemann-Heldt      Moritz Hennemann

## General Literature

- Bjola/Kornprobst (eds.) (2024), Digital International Relations – Technology, Agency and Order
- Bradford (2012), The Brussels Effect, Northwestern University Law Review, Vol. 107, No. 1, 2012
- Bradford (2023), Digital Empires, pp. 1-29, 360-393
- Celeste/Heldt/Iglesias Keller (2022). Introduction. In: Celeste/Heldt/Iglesias Keller (eds.), Constitutionalising Social Media, pp. 1-8
- EU Commission, A European strategy for data, COM(2020) 66 final
- Feakin (2024), Navigating the New Geopolitics of Tech, Harvard Business Review Blog
- Gasser/Mayer-Schönberger (2024), Guardrails – Guiding Human Decisions in the Age of AI, pp. 1-36, 184-191
- Hennemann (2023), Global Data Strategies: An Introduction, in: Hennemann (ed.), Global Data Strategies, pp. 1-10
- Hennemann/Gasser (2023), Unlocking The Potential of the Data Age: Key Tasks and Challenges of Data Strategies, *ibid.*, pp. 11-23
- Rosenbach/Mansted (2019), The Geopolitics of Information
- Schaake (2024), The Tech Coup: How to Save Democracy from Silicon Valley
- The [German] Federal Government (2024), Strategy for International Digital Policy of the Federal Government

## A. Facebook Free Basics (2013 et seq.)

A Free Lunch? – ‘Zero Rate’ and a Fragmented Internet

*Access to the internet by private actors? – new chances, new dependencies? – net neutrality – ‘there is no such thing as a free lunch’ – is limited access by private actors better than no access? – the gatekeepers of the digital world – is there a ‘right’ to internet access?*

- Graham (January 11, 2016). Facebook is no charity, and the ‘free’ in Free Basics comes at a price, TheConversation.com
- Bhatia (May 12, 2016). The inside story of Facebook’s biggest setback, The Guardian
- ECJ, ECLI:EU:C:2021:675, ECLI:EU:C:2021:676, and ECLI:EU:C:2021:677

## B. 5G & Huawei (2016 et seq.)

Power by Hardware?! Or: To Use or Not To Use?

*Who controls the infrastructure, controls...? – what is ‘digital sovereignty’? – cheap technology, expensive (collateral) effects? – China and its role in the Global South – are dependencies in a connected and globalised world inevitable?*

- Moehr (July 23, 2023). My Way or the Huawei: 5G at the Center of US-China Strategic Competition, Atlantic Council
- Berman/Maizland/Chatzky (February 8, 2023). Is China’s Huawei a Threat to U.S. National Security?, Council of Foreign Relations
- Erie/Streinzi (2021). The Beijing Effect: China’s Digital Silk Road as Transnational Data Governance, 54 N.Y.U. J. Int’l L. & Pol. 1

## C. Snowden & Schrems (2013 et seq.)

Public and / or Private Surveillance?

*Data flow 'borders' in the digital world? – data access and data processing in a connected world – surveillance technologies – extraterritorial law enforcement and its trade-offs – data flows and security authorities – how to steer international data transfers and data access – protection of personal data and the global rise of the GDPR – the GDPR's approach as 'Gold Standard' – Brussels Effect (Bradford)*

- Zuboff (2019). The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, pp. 27-62
- ECJ, ECLI:EU:C:2015:650 – Schrems I, ECLI:EU:C:2020:559 – Schrems II
- Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ L 231, 20.9.2023, pp. 118 et seq.
- McCabe/Satariano (May 23, 2022). The Era of Borderless Data Is Ending: Nations Are Accelerating Efforts to Control Data Produced Within Their Perimeters, Disrupting the Flow of What Has Become a Kind of Digital Currency, The New York Times
- Yakovleva (2022). On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows, Legal Issues of Economic Integration, 339-348



## D. China's Social Credit Scoring (2017 et seq.)

Bonus or Minus Miles by the State?

*Reality of and myths about the Chinese Social (and Company) Credit Scoring – rating of societal relevant behaviour – penetration of digital technologies in private lives – datafication of law enforcement – societal measurement and control*

- MERICS (February 11, 2022). China's social credit score – untangling myth from reality
- Damm (March 3, 2022). Chinas Digitalisierung: Effizienz und Kontrolle durch eigene Technologiestandards. Bundeszentrale für politische Bildung
- Liu (2021). The Rise of Data Politics: Digital China and the World, Studies in Comparative International Development, 45-67
- Chander/Sun (2022). Sovereignty 2.0, Vanderbilt Journal of Transnational Law, 283-324
- Wu (July 2021). Sovereignty and Data Localization, Belfer Center

## E. Facebook and the Rohingya Genocide (2017)

How Online Speech Transforms into Real-life Violence

*The interdependencies between social networks and its users – hate speech – extraterritorial effect of the U.S. First Amendment – content moderation and corporate responsibility – social media platforms as neutral intermediaries?*

- Mozur (October 15, 2018). A Genocide Incited on Facebook, With Posts From Myanmar's Military, The New York Times
- Crystal (September 7, 2023). Facebook, Telegram, and the Ongoing Struggle Against Online Hate Speech, Carnegie Endowment for International Peace
- Crockett (2017). Moral outrage in the digital age, Nature Human Behaviour 1, 769-771
- O'Callaghan et al. (2015). Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems, Social Science Computer Review, Vol. 33(4), 459-478

## F. Cambridge Analytica (2016 et seq.)

Microtargeting in Elections' Times and Beyond

*Terms and conditions for personal data use – privacy in times of constant content creation – manipulation via microtargeting – limits between commercial advertising and political microtargeting*

- Cadwalladr/Graham-Harrison (Mar 17, 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian
- Moore (March 20, 2018). Cambridge Analytica Had a Role in Kenya Election, Too, The New York Times
- Bernzen (2023). 'Data Colonialism'? Big Data's Adverse Impact on the (Global) South, In: Hennemann (ed.), Global Data Strategies, pp. 171-186

## **G. Bolsonaro and WhatsApp (2018)**

The Battle for Voters via Private Messaging

*Disinformation via private messaging – democratic risks of disinformation – protecting the electoral process and freedom of expression*

- Evangelista/Bruno (2019). WhatsApp and political instability in Brazil: targeted messages and political radicalization, Internet Policy Review Vol. 8 (4)
- Siapera/Kirk (2022). Social Media, Electoral Campaigns and Regulation of Hybrid Political Communication: Rethinking Communication Rights, In: Celeste/Heldt/Iglesias Keller (eds.), Constitutionalising Social Media, pp. 119-138
- Benkler/Harris/Roberts (2018). Network propaganda: manipulation, disinformation, and radicalization in American politics, pp. 341-349

## H. WeChat & Co. (2018 et seq.)

The Economics and Political Dimensions of All-Encompassing Digital Ecosystems

*'Private Power' and political influence – the network economy and network effects – bottlenecks and lock-in effects – multi-sided platforms and digital ecosystems – 'platformisation' – what kind of 'efficiency' do we seek?*

- Schnurr (2023). Global Data Economics: Principles, Strategies and Policies, In: Hennemann (ed.), Global Data Strategies, pp. 35-49
- Poell/Nieborg/van Dijck (2019). Platformisation, 8 Internet Policy Review, Issue 4
- Sanders (2022). The Rise of Social Media in the Middle East and North Africa: A Zool of Resistance or Repression, In: Celeste/Heldt/Iglesias Keller (eds.), Constitutionalising Social Media, pp. 25-41
- Pałka (2020). Algorithmic Central Planning: Between Efficiency and Freedom, 83 Law and Contemporary Problems 125

# I. De-Platforming Trump? (2021)

Hate Speech and the Storm on the Capitol

*Limits of free speech? – hate speech and ‘borderline’ content – incitement to violence – content moderation – the power of social media platforms – constitutional rights and private actors – the Facebook Oversight Board*

- Jaffer/McGregor/Corpus Ong/Owen/Tworek (Jan 18, 2021). Does Deplatforming Trump Set a New Precedent for Content Moderation?, CIGI
- Kuczerawy (Jan 29, 2021). Does Twitter trump Trump? A European perspective, Verfassungsblog
- Klonick (Feb 12, 2021). Inside the Making of Facebook’s Supreme Court, The New Yorker

## J. Digital Diplomacy (2008 et seq.)

Off the Beaten Track?

*Diplomacy in the virtual world – diplomacy with respect to the digital world – international digital policy – internet governance – internet governance forum – ICANN – WTO – OECD – data diplomacy – multistakeholder governance*

- Lichtenstein (2010). Digital diplomacy, New York Times Magazine, 16(1), 26-29.
- Manor (2018). The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology, DigDiploROx Working Paper No 2
- Clüver Ashbrook (January 14, 2020). From Digital Diplomacy to Data Diplomacy, Belfer Center
- Kleinwächter, W. (2021). Cybersecurity, Internet Governance, and the Multistakeholder Approach, Cyberstability Paper Series

## K. Starlink in the Ukraine (2022)

Access to and Use of the Internet in Times of War

*Public infrastructure and public facilities by private entities – private support and intervention in international armed conflicts – connectivity as a prerequisite for modern warfare – outer space as a ‘field of conflict’ – dual use technologies*

- Jayanti (March 9, 2023). Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?, Belfer Center
- Chullila, J. (Apr 10, 2024). Ukraine Is the First “Hackers’ War”. IEEE Spectrum.
- Thompson, K. D. (Jan 16, 2024). How the Drone War in Ukraine Is Transforming Conflict. Council on Foreign Relations



## L. Scraping Everything (1993 et seq.)

The Political and Economic Chances and Perils of a Fully 'Readable' World

*Privacy – immaterial goods – law enforcement – predictive policing – training of Artificial Intelligence models – public domain data for proprietary tech – who 'owns' the world's (openly available) information? – access to data for research*

- Porter (Feb 6, 2020). Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech, The Verge
- Heldt/Kettemann/Leerssen (Nov 30, 2020). The Sorrows of Scraping for Science, Verfassungsblog
- Balevic (Jun 7, 2024). Meta may have to hit the brakes on its big AI training plans, Business Insider

## M. Google's Gemini (2023)

Generative AI between 'Finding' and 'Creating' New Facts

*Next generation(s) of Artificial Intelligence – large language models – data quality and veracity  
– 'unbiased' tech? – ethics of Artificial Intelligence – 'human in the loop' – access to knowledge  
– digital literacy*

- Grant (February 26, 2024), Google Chatbot's A.I. Images Put People of Color in Nazi-Era Uniforms, The New York Times
- The Daily (March 7, 2024), The Miseducation of Google's A.I., The New York Times
- Gasser/Mayer-Schönberger (2024), Guardrails – Guiding Human Decisions in the Age of AI, pp. 59-80
- Hacker/Zuiderveen Borgesius/Mittelstadt/Wachter (June 26, 2024), Generative Discrimination: What Happens When Generative AI Exhibits Bias, and What Can Be Done About It?, in: Hacker et. al. (eds.), The Oxford Handbook of the Foundation and Regulation of Generative AI, 2024 (forthcoming)

## N. EU Digital Services Act (2022) & UK Online Safety Act (2023)

‘Taking Back Control’? (Part 1)

*The legacy of the German Network Enforcement Act (2017) – risk-based approach – ‘Very Large Online Platforms’ – “Awful but lawful?” – gaining ground in the global regulatory races? – Brussels Effect (Bradford)*

- Raue/Heesen (2022). Der Digital Services Act, Neue Juristische Wochenschrift, 3537-3543
- Heldt (2022). EU Digital Services Act: The White Hope of Intermediary Regulation. In: Flew/Martin (eds.), Digital Platform Regulation – Global Perspectives on Internet Governance
- Helberger/Samuelson (March 7, 2024). The Digital Services Act as a Global Transparency Regime, Verfassungsblog
- Raue/Kwiatkowski (2024). Der UK Online Safety Act (OSA) im Vergleich mit dem Digital Services Act – Was bedeutet „take back control“ bei der Plattformregulierung?, Multimedia und Recht, 133-137

## O. EU AI Act (2024) & US Executive Order on AI (2023)

‘Taking Back Control’? (Part 2)

*The ‘European Way’? – how to regulate Artificial Intelligence? – aims of Artificial Intelligence regulation – economic effects of Artificial Intelligence regulation – non-economic dimensions of Artificial Intelligence – building trust by regulation? – Brussels Effect (Bradford)*

- Chibanguza/Steege (2024), Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, Neue Juristische Wochenschrift, 1769-1775
- Novelli/Casolari/Hacker/Spedicato/Floridi (March 21, 2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity
- Dougall/Ostrowski (Jan 3, 2024). What’s in Biden’s Executive Order on Artificial Intelligence?, Lawfare
- Susarla (Nov 2, 2023). Biden administration executive order tackles AI risks, but lack of privacy laws limits reach, The Conversation

## **P. Metaverse (2023)**

The Immersive Worlds We (Might) Live In

*Building immersive worlds – global communication networks – networks for all senses? – private ordering and state control? – becoming the gatekeeper of gatekeepers? – multiple (interoperable) metaverses? – in how many worlds do we live?*

- Herrman/Browning (July 10, 2021). Are We in the Metaverse Yet?, The New York Times
- Clegg (May 18, 2022). Making the metaverse: What it is, how it will be built, and why it matters, Medium
- Kettemann/Müller/Böck (2023). Regulatory approaches to immersive worlds: an introduction to metaverse regulation, Project Immersive Technology

## Q. Rise and Fall of FTX (2023)

Creating New Values, Creating New (Systemic) Risks?

*Realities and opportunities of as well as myths about the Blockchain – cryptocurrencies — fintechs – funding innovation, supporting fraudulent business models? – systematic risks – overcoming traditional intermediaries by new ones?*

- Oliver (February 9, 2023), 'Sam? Are you there?!' The bizarre and brutal final hours of FTX, Financial Times
- Khalili (Nov 9, 2022). What the Hell Happened to FTX?, Wired
- Spiegel Original Podcast (2023). Krypto-Guru, Der Spiegel
- World Economic Forum (May 2023). Pathways to the Regulation of Crypto-Assets: A Global Approach. White Paper

## R. ‘Pay Or Consent’ (2024)

Brave New (Digital) World?

*Regulating gatekeepers in digital markets – EU Digital Market Act (2022) – the ‘value’ of personal data – tracking users for ad-based business model – the ‘attention economy’ – micro-targeting – privacy – the interplay between competition (law) and data protection (law) – Brussels Effect (Bradford)*

- ECJ, [ECLI:EU:C:2023:537](#)
- [European Data Protection Board \(2024\). Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms](#)
- [EU Commission \(March 25, 2024\). Press Release: Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act](#)
- [Zimmer/Göhl \(April 10, 2024\). Enforcement of the Digital Markets Act – The European Commission Takes Action](#)

## S. Worldcoin's Iris Scanning (2024)

The Transparent Citizen or: Humankind's Metrification

*Cryptocurrencies – digital identity and digital identities – a 'private' census? – privacy – which data do we (not) want – how much transparency is possible and desired? – individual and commonwealth effects – trade-offs of metrification*

- Nieva (August 10, 2023). Sam Altman's Eyeball-Scanning Crypto Project Worldcoin Is Having An Identity Crisis, Forbes
- Howcroft (July 31, 2023). "France's watchdog questions legality of Worldcoin biometric data collection", Reuters
- Giannopoulou, A. (2023). Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity, DISO 2, 18



## T. Deep Fakes (2023)

Do You Believe Your Own Eyes?

*Democratic risks of disinformation – protecting the electoral process and freedom of expression  
– pros and cons of synthetic media – recalibration of human Interaction and influence in the 21<sup>st</sup>  
century – whom do we trust? – Artificial Intelligence against and / or for democracy?*

- Ray (December 18, 2023). Imran Khan—Pakistan’s Jailed Ex-Leader—Uses AI Deepfake To Address Online Election Rally, Forbes Middle East
- Shukla/Schneier (June 10, 2024). Indian election was awash in deepfakes – but AI was a net positive for democracy, TheConversation.com
- Unzicker (August 10, 2023). Disinformation – A Challenge for Democracy

## Contact Details

Dr. Amélie Hennemann-Heldt  
Leibniz-Institute for Media Research  
Rothenbaumchaussee 36  
D-20148 Hamburg  
a.heldt.ext@leibniz-hbi.de  
<https://leibniz-hbi.de/en/>

Prof. Dr. Moritz Hennemann  
University of Freiburg Law Faculty  
Institute of Media and Information Law, Dept. I: Private Law  
Rempartstraße 4  
D-79098 Freiburg  
moritz.hennemann@jura.uni-freiburg.de  
<https://uni-freiburg.de/jura-medienrecht>