INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

SPECIAL ISSUE

OPEN ACCESS

From trust in the system to trust in the content

Péter Mezei *University of Szeged* mezei@juris.u-szeged.hu
Andreea Verteș-Olteanu *West University of Timișoara* andreea.vertes@e-uvt.ro

DOI: https://doi.org/10.14763/2020.4.1511

Published: 21 October 2020
Received: 31 August 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Mezei, P. & Verteș-Olteanu, A. (2020). From trust in the system to trust in the content. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1511

Keywords: Trust, Internet, Association of Internet Researchers

Abstract: The internet is the digital reincarnation of a Greek agora or a Roman forum. It works as a “place” for public and private life. As such, it requires reliable, trustful rules to govern the daily routine of its visitors/users. The governance of the internet has gone through a significant (if not tectonic) change since its standardisation. This is clearly reflected by the changes in the concept of trust as well. Historically, trust reflected the concerns of internet users regarding the intrusion of governments into the neutral functioning of this “place”. As of now, concerns regarding trust are equally present at the macro and micro level. Trust in platforms and in the content made available through the internet is at the centre of disputes nowadays. This editorial intends to provide for a selected introduction of the macro- and micro-level aspects of trust in the system and trust in the content, including content moderation, copyright law, fake news, game-making, hateful materials, leaking, social media and VPNs.

PAPERS IN THIS SPECIAL ISSUE

EDITORIAL

From trust in the system to trust in the content

Introduction

Back in 1996, the cyber libertarian political activist John Perry Barlow published his Declaration of the Independence of Cyberspace. He started his declaration as follows: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (Barlow, 1996). We shall agree with van Dijck and Rieder that "[w]hile the mythos of cyberspace as a new frontier has long faded, common terms like 'internet culture' or even 'online shopping' signal that there is some kind of *elsewhere* in the clouds behind our screens" (van Dijck and Rieder, 2019, p. 3). The internet is such an *elsewhere*: a digital reincarnation of a Greek *agora* or a Roman *forum*. It works as a "place" for public and private discussions, debates, meetings, *rendez-vous*. It is a marketplace. And such a place requires reliable, trustful rules to govern the daily routine of its visitors/users.

What makes Barlow's declaration a relevant reference point for this editorial is nothing else than to signal that it was a clear warning to the governments of the world that users of the new medium, the internet, do not trust them. Users feared that governments intend to limit the use of the internet just as they posed significant limitations to the liberties of children for example. He continued: "you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace" (Barlow, 1996). The internet has since transformed into a more robust system that can only be analysed in an interdisciplinary way (Consalvo and Ess, 2011). Likewise, trust in the system has transformed into a more complex metaphor: covering not only (dis)trust in governments, but (dis)trust in other users, intermediaries, platforms, data, information and news etc. In sum, *trust in the content*.

The *Association of Internet Researchers* (AoIR) is a leading global organisation to enhance the interdisciplinary research of internet studies. It organises its annual conferences since two decades, and centres these events around a specific topic since 2016. The latest edition of this conference series took place in Brisbane, Australia. The October 2019 event intended to "explore the question of whether we can still have, or how we might regain, trust in the system: in a world of unscrupulous actors and dubious data, how can we know what and whom to trust? Indeed, how might we change the system itself–rethinking, redesigning, rebuilding, repurposing it – to provide a more trustworthy experience for a broader, more diverse, more inclusive community of Internet users?” (Association of Internet Researchers, 2019). Hundreds of excellent papers analysed the macro and micro level aspects of trust in the digital environment.

Internet Policy Review, a leading open access journal for interdisciplinary internet research, collaborates with AoIR since 2018 to publish hand-picked peer-reviewed articles by participants of AoIR conferences. This special issue is the third in this row (Dutton, 2018; van Dijck and Rieder, 2019), and trust in the system, as a topic, fits perfectly into the mission of the journal: it is inherently interdisciplinary, policy oriented and it is a really hot topic of internet research.

This editorial is structured as follows. First, we’ll address trust at a macro level: its meaning and its relevance in our digital society. Second, we’ll introduce three cherry-picked micro level aspects of trust (in the system): fake news, leaking and copyright law. The selection of these aspects is twofold. On the one hand, they meet the scientific interest of the authors of this editorial. On the other hand, this editorial intends to work as an addendum to the papers selected and peer-reviewed for this special issue. More precisely, the editorial discusses aspects of trust that the selected papers mainly miss to analyse. Third, the editorial ends with the short introduction to the six contributions presented originally at AoIR 2019, and developed later into peer-reviewed articles.

Trust

Law is a fiction (Fuller, 1967; Del Mar and Twining, 2015). Unlike rules of nature (e.g., gravity, H^2O and so forth), laws are created and recreated by humans in order to describe and reflect social realities. Ideally, the final goal of law is to guarantee the functioning of the whole society. Legal concepts reflect physical realities (e.g., ownership is historically bound to tangibles) and metaphysical phenomena (e.g., some countries guarantee ownership interests over intangibles). The legal reflection of these concepts might change from time to time. What is lawful today might become illegal later on and *vice versa*. Brand new social, economic and technological challenges lead to regular reformulations of the law.

Laws do not only aim to guarantee social stability and reliability, but they shall pursue the goal of benefiting all humans (not to mention others, e.g., animals or the environment in general) rather than discriminating against minorities. The fate of the rules is heavily affected by the fact of whether or not they are accepted and followed by their subjects. The best laws are those that we follow since we understand and agree with them - we trust in them. Some of the laws are obscure, they are based on flawed policy arguments, outdated or simply unnecessary. Noone denies that parents shall be liable for the damages caused by their infant children. It, however, changes from time to time what an infant might be able to do: stealing daddy's car seems to be physically more troublesome (and hence more controllable) than texting a bully on a smartphone. Similarly, while the majority of society understands why stealing a car is against the law, a significant part of society thinks it is unfair to prohibit (and also criminalise) the unauthorised downloading of copyrighted contents through P2P file-sharing platforms. If laws regulate against social norms, the acceptance and the following of, as well as the trust in law, erodes or disappears.

Metaphors are commonly used in law (Larsson, 2017). They are capable of defining realities (Lakoff and Johnson, 2003, p. 157) and helping "the imaginary become real or true" (Wyatt, 2004, p. 244) Metaphors "create cognitive bridges between disparate subjects, mapping existing knowledge about a familiar and concrete source domain onto unfamiliar, abstract, or novel concepts" (Gill, 2018, p. 454.), and their main task is to persuade people (Fuller, 1930, p. 380) Metaphors strengthen the rationale of any given rule, or support the understanding of a norm by attaching an already existing expression (often legal terms) to a phenomena, and hence providing existing knowledge to emerging legal questions. As Gill explained, "[t]he metaphors chosen by a court or legislature will effectively determine the validity of certain arguments, delimit the boundaries of acceptable debate, and reshape what we understand to be both 'logical' and legal in a given situation" (Gill, 2018, p. 456). Metaphors have a vital role to describe technological challenges, too. This is mainly due to the constant development of technology and the pace of it, as well as to the fact that "the digital" is formless, that is, metaphors are more necessary to describe realities than tangible/material/analogue elements of society (Gill, 2018, p. 457).

Notable metaphors - including "skeumorphs", that is the reused versions of old concepts (Larsson, 2011) - in the digital domain of law are for instance cyberspace, information superhighway, singularity, the cloud, transparency, net neutrality, piracy, big data, raw data, data mining, harvesting, artificial intelligence, domain (name), platform, (safe) harbour, bulletin board, torrent, search engine, magnet link, swarm, virus, Trojan horse, leak, or - as discussed in this special issue - 'going dark' to describe the risks of end to end encryption (Heemsbergen and Molnar, 2020).

Metaphors are also used to link new technologies to existing rules (Gill, 2018, p. 457). As Tim Hwang and Karen Levy noted, "[a]s technology advances, law evolves (slowly, and somewhat clumsily) to accommodate new technologies and social norms around them. The most typical way this happens is that judges and regulators think about whether a new, unregulated technology is sufficiently like an existing thing that we already have rules about—and this is where metaphors and comparisons come in" (Hwang and Levy, 2015). The main purpose of such metaphors in law and technology is to guarantee that the conceptualisation, the regulation, the administration and the use of the new technology goes smoothly.

Trust is an important metaphor. In some sense, trust means the freedom of giving up the obligation of experimenting, learning and acting individually. At the same time, it also represents the acceptance of the specialised society, that is, that we are neither able nor obliged to know and do everything on our own; we can rely on others who have the relevant knowledge or who are able to do the given task, and we shall trust in and follow their decisions. Balázs Bodó defines trust on an interpersonal level "as the willingness to cooperate with another in the face of uncertainty, contingency, risk, and potential harm" (Bodó, 2020, p. 2.)

Trust in the system has its own metaphorical meaning. In conjunction with trust's metaphorical meaning, it requires internet users to accept and follow the rules of the web, and, for the less e-literates, to stick to the options available online (including but not limited to platforms).

The 'Barlow fears' from government misuses gave place to cybersecurity concerns in the early years of the internet. The financial motives of cybercriminals as well as the pure dangers of cybercrime grew along with the economic growth of the internet. Frederick Chang noted that "[h]umans must defend machines that are attacked by other humans using machines" (Chang, 2012). Cybercrimes and information security thus evolved together (Bauer and van Eeten, 2009, pp. 707-710). The growing popularity of cyber attacks was mainly due to their cheap, convenient and less risky nature (Jang-Jaccard and Nepal, 2014, p. 973). Viruses, Trojan horses, worms, bots or spyware pose a significant threat to reliability of and trust in the system by, just to name a few, online identity or data thefts, phishing or industrial espionage (Moore, 2010, pp. 104-105).

It is, of course, not only illegal financial motives that might threaten the trust in the system. Web 2.0 led to a hyper-atomised internet: the actors and their possibilities of data creation, dissemination and access were multiplied and polarised. Intermediaries/platforms emerged and provided the means and space of participatory culture (e.g., on YouTube's role see Burgess and Green, 2018). These platforms turned to be the main engines of the internet economy and platform capitalism.

They, however, do not intend to solely serve social interests. Corporate financial motives are in the end the drivers of decisions by platform operators.

The internet has become the forum of personal opinions, the "*elsewhere*" of artistic, spiritual and political life. As data has become a leading source of revenue and power, the reliability of data, its creator and disseminator has become a preeminent concern. Trust in the system started to include trust in the content, its creator and its disseminator. At the same time, platforms are the new capitalistic enterprises, with their own values and private norms. Trust in these platforms is the foundation of their reliability and functioning. How they react to social events becomes crucial. The role that platforms played during the Arab spring, the #MeToo or #BlackLivesMatter campaigns; how Twitter labelled President Trump's tweet as misleading (and how Facebook disagreed with the rival platform for a while) following the outrage sparked by the death of George Floyd Jr. (Newton, 2020); or how President Trump proclaimed a regulation to punish social media platforms for such labelling (Heldt, 2020) are excellent examples for the role that platforms play in deteriorating, preserving or strengthening trust in the system and content.

The issue of trust in the system is present in the micro-level of the internet, too. This editorial, before turning to the actual papers selected for this special issue, intends to highlight the importance and the consequences of (the lack of) trust in three micro-fields of the internet: fake news, leaking and copyright law.

Fake news

Good and ethical journalism is based on trust, developed from the assumptions that the communicated news reports are true and the information is reliable, accurate and trustworthy. The basic responsibility of a journalist is to seek, publish, and, above all, respect the truth. However, in an ever-growing digitalised world, media consumers are involved in an unprecedented transfer of information and, as a result, the trust paradigm is in considerable danger. Truth is being replaced by *post-truth*, and story news by *fake news* (Palczewski, 2017).

'Journalistic deception' was defined as an act of communicating messages not only by lying, but also by withholding information, so as to lead someone to have a false belief (Elliot and Culver, 1992). However, despite its deeply troubling recent online development, the spread of false news and journalistic deception dates back to antiquity. Mitchell Stephens offers the example of *Acta Diurna*, a proto-newspaper of 47 AD, where the author of disinformation was none other than Pliny the Elder, the renowned Roman savant, naturalist and natural philosopher

(Stephens, 2007, p. 57). In 1747, Benjamin Franklin did the same, in an article written for the *London General Advertiser.* He published the statement of a young mother, Polly Baker, accused of extramarital sex. The speech was supposed to have made such an impression on the jury, that they acquitted her of the charges. Thirty years later, Franklin admitted that he had invented Polly Baker (Kitty, 2005, p. 227). False news existed before the Gutenberg press and flourished afterwards, simply because, just as information wants to be free, so does misinformation. The printing press empowered reformers alongside hawkers, profiteers, and bigots. The invention of the printing press simply shifted the problem of the gatekeepers of truth, aka the information: the old gatekeepers were princes and priests. The new ones were entrepreneurs such as Gutenberg or Caxton (Marantz, 2019).

Despite the coining of the term *fake news* in the mid-2010s, propaganda, misinformation, disinformation, and all types of news hoaxes have for long been present in the history of the world and called bias, spin or lies. They caused, not always directly, international incidents, even wars, such as the Spanish-American War of 1898, the Gleiwitz incident of 1939, Vietnam, the Second Iraqi War (Palczewsi, 2017), and often originate with totalitarian dictatorships, though one can easily spot politically driven hoaxes even in democratic countries, especially when faced with electoral campaigns (e.g., Viktor Orbán in 2018 or Boris Johnson in 2019).

In a nutshell, fake news is intentionally fraudulent, aimed to deceive the receiver, often with an underlying objective to achieve a certain material, political, personal, or group gain or simply to entertain or excite.

From a theoretical point of view, there are seven identifiable types of fake news: false connection (when headlines or visuals do not support the content), false context (when genuine content is shared with false contextual information), manipulated content (when genuine information is manipulated to deceive), satire or parody (no intention to harm), misleading content (misleading use of information), imposter content (when genuine sources are impersonated) and fabricated content (content that is 100% false, designed to deceive and do harm) (Wardle, 2017). Additionally, we have Melissa Zimdars' classification of fake information, which determines which category a website may occupy: fake news, satire, extreme bias, conspiracy, rumour mill, state news, junk science, hate news, clickbait (Zimdars, 2016).

Irrespective of the form, today's online platforms totally reshaped the spread and potential impact of fake news on people's lives, behaviour and mentality. It became an indispensable element of the digital landscape. Its influence on public opinion is considerably bigger than that of real news stories and the explanation is simple and bitter: 1. large dissemination equals authenticity and 2. the influence of lies exceeds that of the truth. “Repeat a lie often enough and it becomes the truth” is a manipulation principle misattributed to Nazi politician and Reich Minister of Propaganda, Joseph Goebbels (Schultze, Bytwerk, 2012, p. 217), but still accurate, irrespective of its true author. Fake news reports are, in the digital age, repeated, processed, tweeted and propagated through various online channels and end up acquiring the markers of ‘authenticity’ (Palczewsi, 2017). They have a tremendous potential to mobilise people. Furthermore, we must admit that they tend to be more seductive. In the words of Friedrich Nietzsche, “the champions of truth are hardest to find, not when it is dangerous to tell it, but rather when it is boring” (Nietzsche, 1996). Or, to put it bluntly, “there is nothing as boring as the truth” (Bukowski, 2001). Fake news draws the public’s attention through its attractiveness; it lures the receivers by offering them something that matches their views, beliefs and expectations.

The fact that fake news has become a constant element in the media-created landscape is also linked to the fact that not only the media have changed, but also their audiences. The public for news and information is now hyper-atomised, far beyond the traditional media, in the form of billions of one-person audiences that often double as disseminators of the same information (Gross, 2017). We are the furthest away from Bertolt Brecht’s “literature without consequences” (as he perceived *radio* to be: „radio is one-sided when it should have two sides. It is a pure instrument of distribution; it merely hands things out.”), which fails to make contact with its audience, and in which the public is, in fact, a mass of people, voiceless and inactive (Brecht, 1979, p. 25). The digital (just like Brecht’s ideal *theater*) allows for a multi-way conversation, in which the audience creates a liquid communication world, as part of the ‘liquid modernity’ described by Zygmunt Bauman. The individuals live fragmented lives, with the institutions and social forms around them constantly changing and providing little in terms of frames of reference and long-term plans (Bauman, 2000).

The internet revolution has transformed the consumer of information into a generator of content. This shift has brought along another change as well: as we enter the post-trust era, facts and evidence have been replaced by personal belief and emotion. Consequently, the nature of news, and what people accept as news, is slowly but steadily transforming into an emotion-based market. The truth of the story no longer matters. What matters is that the story falls in line with what a person wants to hear. Fake news no longer means factless, libellous or simply false news, but rather news that is seen to attack a person’s pre-existing beliefs.

This is the truth of the post-truth era (Rochlin, 2017).

This danger goes hand in hand with the audience's ease to accept, embrace and readily disseminate this new 'truth': Nick Rochlin goes on to show that the majority of people don't read beyond an article's headline (Rochlin, 2017). Moreover, a study by Maksym Gabielkov and colleagues (2016) showed that 59% of the news articles that are shared on Twitter aren't even read before they're shared (Gabielkov et al., 2016). Yoonmo Sang and colleagues recently highlighted that "there is a positive correlation between frequency of news use and interest in news and trust in news. (…) Not only do perceptions of trust influence a person's news consumption, studies show it also has an impact on how they interact with it. Based on a large-scale survey on news consumption in 11 countries, (…) showed that those who had low levels of trust in the news media were more likely to share or comment on online news and prefer non-mainstream news sources, such as social media outlets, blogs, and digital native sources, such as The Huffington Post, than people with higher levels of trust in news" (Sang et al., 2020, pp. 4-5). Unlike traditional media sources, the social platforms allow their users to create a bubble of news stories that strike a chord only with their own pre-defined beliefs and opinions. And since the majority of users trap themselves in their own bubbles, full of niceties and one-sided points of view, contemporary society is faced with peril of yet ever more rigid beliefs and deep societal fissures. This inclination to select the media outlet which best aligns with their preconceived attitudes is in line with Joseph T. Klapper's selective exposure theory, which suggests "the individuals' tendency to favour information that reinforces their pre-existing views while avoiding information that is contrary" (Klapper, 1960). When a mismatch of contradictory beliefs occurs, individuals find it 'inherently dissatisfying' and so they seek out information that is based on their own beliefs, perspectives and attitudes (Hart et al., 2009). In the age of social platforms, people are no longer inclined towards emphatic receptivity; they are losing their openness and availability to listen to others' different opinions.

The gatekeepers have changed, once more. The agenda setting is no longer in the sole hands of owners, publishers, editors and directors. The digital media are not the gatekeepers of old (Gross, 2017). Groups and individuals, with direct access to audiences, have taken control of the terms of public discussion and their criteria for the selection of information is based entirely upon their own interests and biases. Jürgen Habermas' public sphere (traditional and bourgeois) is gone. Today's curators of information are individuals and technology companies. The controller has changed, but the problem remains the same, namely the threat to liberal democracy everywhere. While waiting for possible solutions to counterbalance the effects and influences of digital media on our day-to-day existence, negative emotions, (political) thoughts and social behaviour, on- and offline, we must acknowledge the fact that fake news is already part of our reality, one with which we will have to learn to coexist.

Leaking

Democracy means (indirect) self-government by the people. For such a system to work, an informed electorate is crucial. Democracy cannot work if those in power manipulate the electorate by withholding information and suppressing criticism. Freedom of expression is intimately linked to political debate and the concept of democracy. Free speech is multifaceted, and includes the right to seek, receive and impart information and ideas (Milton, 1918). In a democracy, people need access to information (be it political, social or economic in nature) in order to decide whether their elected officials are acting in the public interest or not. However, far too often, politicians evade such scrutiny, allowing fraud and abuse of power to go unhampered. So we ask ourselves: how far can the freedom of expression go so as not to infringe national interests? In the end, which of the two prevails, the freedom of the press or national security? Can the "need to know" cross boundaries and break laws? Ever since its foundation, WikiLeaks, a website devoted "to bringing important news and information to the public" (according to its own description), has become a major source of freedom of knowledge and, due to its alliance with major print publications, a credible source for leaked information. Whistle-blowing platforms (the roots of which are to be found in WikiLeaks) are increasingly becoming a common tool in journalism, and are one of the strategies that journalists can adopt in communicating with whistle-blowers in a safer way and to obtain data and information without exposing sources to the risk of being identified, tracked, exposed or put in danger (Di Salvo, 2020). Yet, several questions remain, questions of both moral and ethical nature, that deserve close attention: whistle-blowing and leaking obviously come from our desire to know the truth, but does mankind actually deserve full "transparency"? And, in this scenario, are the leakers of information to be perceived as heroes or villains?

State secrecy is enshrined in probably all constitutional texts. Etymologically, 'secret' comes from *secretum*, that which is separated. This separation is between those-who-know and those-who-do-not-know but *suspect* something (Horn, 2011). But does secrecy actually threaten democracy? It is the fear brought by the awareness of not knowing, rather than the content of the secret itself, which matters and jeopardises liberal democracies. State secrecy is vital for national security, but it can also be used to conceal wrongdoing. Are there means to ensure that this power is used responsibly? The problem arises when establishing the instruments that might be used in order to check that such secrets are handled in a responsible manner by those in power. The aim is to ensure that the official justifications for secrecy are sufficiently reasonable and detailed in order to deter overzealous concealment. The abuse of secrecy and leaking are nothing new; the phenomenon is merely augmented by the immense dissemination possibilities of the digital age. However, also characteristic for this new era are conspiracy theories, misdirection, power plays, deflection, allegations of fake news, and fears of pervasive government surveillance (Marcus, 2017), which conclude in any scandalous information and which are then being received by the public with great skepticism.

Rahul Sagar, in his book *Secrets and leaks: the dilemma of state secrecy*, asks himself (and answers) the following question: when can whistle-blowing and leaking be a legitimate means of guarding against the possible harms of executive secrecy? It is important first of all to try and distinguish whistle-blowing from leaking.

Whistle-blowing is usually defined as the activity of calling attention to wrongdoing, an act intended to call out, but also to halt wrongdoing. It is a distinct act of dissent (Elliston et al., 1985), a special form of dissidence in which “a member or former member of an organization goes outside the organization or outside normal organizational channels to reveal organizational wrongdoing, illegality, or actions that threaten the public” (Petersen and Farrell, 1986, p. 5). It typically involves inside informants who want to expose “actual nontrivial wrongdoing” by collaborating with the media (Johnson, 2003, pp. 3-4). The term, coined by US civic activist Ralph Nader in 1971, was meant to avoid the negative connotations associated with words such as informant, squealer, tattletale, betrayer, traitor, rat, weasel, etcetera. However, whistle-blower is not a universally recognised denomination, easily translatable into other languages. The colloquialism, invoking old-fashioned images of a police officer chasing after a lawbreaker, has evolved to mean someone who speaks up when most people do not. Yet, the difficulty in translating the term into other languages has led to problems regarding the whistle-blowers’ public perception. In many EU countries, alternative terms such as “informant”, “denunciator” and “snitch” are still commonly used by citizens and the media alike, continuing to cast whistle-blowers in a false or negative light. The following are some of the translations used throughout the EU, negatively connotated terms being prevalent: *práskač*–snitch–negative (Czech), *sladrehank*–snitch–negative (Danish), *vilepuhuja*–whistle-blower (“piper”)–negative (Estonian), *Nestbeschmutzer*–one who dirties their own nest–negative (German), *corvo*−crow−negative or *delatore*−leaker−very negative (Italian), *chibo / bufo*−snitch−negative (Portuguese). In contrast, we have the Italian *sentinella civica*−civic sentinel, and the term introduced by the Romanian legislation in the field, *avertizori de integritate*−those who give integrity warnings (Worth, 2013, p. 19).

Whistle-blowers are "born, not made" and generally driven by moral conviction or moral narcissism (Sagar, 2013). A whistle-blower is usually cast in a positive light. As Daniel Ellsberg, the former US military analyst who released the 'Pentagon Papers' to the *New York Times*, puts it this way: "Telling the truth, revealing wrongly kept secrets, can have a surprisingly strong unforeseeable power to help end a wrong and save lives" (Ellsberg, 2002, p. 4) (Thorsen, Sreedharan, and Allan, 2013, p. 102).

Most big whistle-blowing stories involve a revelation: fraud, where it may not have been suspected; systematic waste unseen by the public and unnoticed by overseers; abuse of power that we couldn't have even imagined (Gessen, 2019). In the book *Crisis of Conscience*, the author Tom Mueller - a journalist - traces the evolution of the whistle-blower in the American imagination, "from squealer to hero" in roughly half a century. But the repercussions of whistle-blowing, whether in the nineteen-sixties or the two-thousands, as described in the book, are similar: whistle-blowers are fired, ostracised, libeled, stripped of security clearances, denounced as anti-American, and threatened with lifetime imprisonment (Mueller, 2019).

We have as examples the arrest and incarceration of Bradley/Chelsea Manning (the US soldier who leaked a video of a US Apache helicopter murdering several Afghani citizens and two Reuters news reporters) and the further development of how a leaker's mental health and sexual orientation can become the focus of the media and public debate. Edward Snowden (NSA administrator and ex-CIA employee who leaked information regarding the agency's misuse of power by collecting data from several US cellular carriers) was granted temporary asylum, first in Hong Kong, then in Russia, after his global surveillance disclosures ever since 2013, with the US constantly asking for his extradition. Julian Assange, the Australian editor and publisher who founded WikiLeaks in 2006, took refuge in 2012 in the Embassy of Ecuador in London, where he remained for almost seven years. In 2019, in addition to other accusations, the US government charged Assange with violating the Espionage Act of 1917. As of April 2019, he has been incarcerated in a London prison, where he is alledgedly exposed to "psychological torture or other cruel, inhuman or degrading treatment or punishment", according to Nils Melzer, UN rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Melzer, 2019). Even before the digital age, *Deep Throat*, the informant behind the Watergate scandal, and Daniel Ellsberg, the leaker of the Pentagon Papers, represent two major figures in the US espionage and leaking history, either vilified or heralded for their actions.

Europe has its own examples. In 2011, the European Court of Human Rights passed judgment on *Heinisch v. Germany* (28274/08) and ordered Germany to pay damages of €15,000 to Ms Heinisch for infringing her right to freedom of expression, after the German courts upheld her dismissal without notice on the grounds that she lodged a criminal complaint against her employer. The case of nurse Brigitte Heinisch, fired from her job at a nursing home in 2005 after she exposed poor care of some of the residents, illustrates how Germany's legal system does not go far enough to protect whistle-blowers. The case did trigger a political discussion in Germany regarding a statutory whistle-blowers' protection, but although all political parties agreed that whistle-blowing could be a valuable instrument to fight corruption, no actual steps were taken (Thüsing and Forst, 2016, p. 14).

In another oft-quoted example, dating back to 2010, an estimated 800 million litres of caustic red sludge poured out of a reservoir at a Hungarian alumina processing plant, in what is known as Hungary's worst environmental catastrophe. At least seven people died, hundreds were injured or forced from their homes in several villages, and tens of millions of euros in private property was destroyed. Some employees at the plant knew about impending problems with the reservoir, but the company's manager threatened to fire them if they appealed to the authorities. Hungary still lacks an agency where whistle-blowers can report wrongdoing (Worth, 2013, p. 51).

Although Romania became one of the first countries in Europe to pass a standalone and innovative piece of whistle-blower legislation (2004) and is, therefore, very strong in theory, it is equally weak in practice. In 2009, whistle-blowers reported to the National Integrity Council and Transparency International Romania alleged irregularities involving (ironically) four managers of the National Integrity Agency (ANI). Among the allegations was that ANI's chairman was in a conflict of interest by also owning two private companies. Following the report, two whistle-blowers were dismissed from ANI. One prevailed in a court case and was reinstated, but was later dismissed again (Worth, 2015, p. 52).

Despite the specific value of whistle-blowers in exposing and preventing corruption, only four EU countries have legal frameworks that are considered to be advanced: Luxembourg, Romania, Slovenia and the United Kingdom (UK), notwithstanding their flaws in application, as seen in the previous example. In order to overcome this problem and to guarantee a EU-wide standard for the protection of whistle-blowers, the European Union adopted a regulation for whistle-blower protection in December 2019, the Whistle-blowing Directive or Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. The EU member states will be obliged to implement the directive into their own national laws until 2021.

Continuing Rahul Sagar's thought, and as seen in the eye-catching examples mentioned above, we should also take into account the 'retaliation' aspect. Though whistle-blowers act as a sort of institutional 'fire alarm', is it reasonable for us to depend only on those whistle-blowers courageous enough to expose themselves to the public, as well as the authorities, and thus subject themselves to various forms of scrutiny (from their employer/'the state', the judicial, the media, the public, etc.)? Therefore, the more realistic scenario is one involving anonymous leakers. The difference, thus, between a whistle-blower and a leaker is that the identity of the latter is not revealed. The direct result is that, generally, leakers don't suffer the kind of reprisals whistle-blowers do. And since some leaks may be vexatious in nature and not necessarily in the public interest, the issue of trust emerges once more.

In the practice of leaking, *trust* appears two times: firstly, associated with (and triggered by) the lack of trust in politicians and secondly, the trust in the voluntary disclosure of a whistle-blower whose main motive is altruistic, with the only aim of halting some wrongdoing. The problem with trust is that it is extremely difficult to establish and maintain and perhaps nearly impossible to recover once violated. Leaks nowadays are no longer limited to big stories. They have gradually become an essential element of journalism, especially political and corporate. The strong reliance on anonymous sources has intensified the public mistrust of leaking, as well, corroborated with the fact that, if in the recent past, leaks were just a first step in the long and tiresome process of investigative journalism, it is now part of a hyperactive daily news cycle (Marcus, 2017).

Just like in the case of *fake news*, previously discussed, we obsessively return to the idea that what the public needs is well-trained, deontological journalists, capable of gate-keeping information in order to guarantee the availability of accurate information to the public and to prevent undue harm. To put it briefly, trust in the media is only accomplished when media independence is achieved, meaning freedom from any external control or the influence of others (political power, sources of information, media owners, internal constraints, financing sources, pressure groups, etc.). Trust requires a moral component - the fiduciary duty - that develops between professionals who can provide a social good (in this case, the delivery of information) and members of a society who desire that particular good. Furthermore, trust becomes cardinal in this equation when the goods to which we want predictable access (freedom of expression and of information) are increasingly important, as is the case here. And trust is gained when exercising one's profession with 'virtue ethics' (that is morality and fairness, competence, objectivity and accuracy, lack of bias, etc.) and 'being Aristotelian', namely learning to correctly apply Aristotle's Golden Mean or golden middle way (Quinn, 2018).

To return to Rahul Sagar's initial question, there are certain instances in which officials, reporters and publishers should put themselves in harm's way by infringing the law and disclosing classified information. Sagar envisages five conditions that must be met simultaneously in order to justify such an act.

> First, the disclosure must reveal the violation of 'shared interests' insofar as the executive has exceeded lawful authority or established norms. Second, the evidence for wrong doing should be 'clear and convincing'. Third, the threat of this wrong doing must be 'specific and immanent'. Fourth, the official should use the 'least drastic means' of revelation by, in the first instance, whistle-blowing within the organization. Finally, the whistle-blower must be willing to disclose her identity. This is essential to ensure that the whistle-blower is not 'the partisan or the zealot' acting to further sectional or personal interests. (Sagar, 2013, pp. 127-136)

In order to summarise the role and importance of WikiLeaks, and leaking in general, in today's world, we can look at a brilliant interview given before a live audience in London, in 2011, by the Slovenian philosopher Slavoj Žižek, "the Elvis of cultural theory" in the words of the *New York Times*.

> Maybe we learned nothing new, but it's the same as in that beautiful old fairytale, The Emperor's New Clothes. We may all know that the emperor is naked, but the moment somebody publicly says, 'The emperor is naked', everything changes. This is why, even if we learned nothing new–we did learn many new things–but even if nothing is learned, the forum matters. (…) You [WikiLeaks] are–that's why it aroused such an explosion of resentment–not only violating the rules, disclosing secrets. Let me call it in the old Marxist way: The bourgeois press today has its own way to be transgressive. Its ideology not only controls what one says, but even how one can violate what one is allowed to say. So you are not just violating the rules. You are changing the very rules how

> we were allowed to violate the rules. This is maybe the most important thing you can do. (Brevini et al, 2013, p. 257)

We must learn to accept the constant battle between state secrecy and unauthorised leaks. The proper security of a country can be guaranteed only with an adequate balance between keeping secrets in order to protect the population from various types of threats and uncovering secrets in order to guard against those powers which have acted *ultra vires*.

Copyright law

Copyright law perfectly indicates the complexities and fallacies of trust in the system. This field of law arose at the junction of technological development (the moveable type printing press developed by Gutenberg), the rise of individualism (especially during the Italian renaissance) and the growing social demands for cultural expressions.

For a long period of time, copyright law has developed at a constant pace, but limited the entering of ‘disseminators’ territory. The ‘read-only’ culture, as coined by Lessig (2008), dominated copyright’s domain until the late 19th and early 20th century. Since then, with the advent of ‘read/write’ culture, the rapid technological developments (especially those related to audio- and audiovisual works, the mechanical dissemination of contents, e.g., radio, television, and later on digital technologies, especially the internet) as well as society’s instant adherence to the new tools and features, has forced copyright law to face its greatest challenge ever. The trust in the social value and relevance of copyright protection is at stake. Copyright law’s structure, logic, policy considerations, and its exact rules (especially the term of protection, or the balance of exclusive rights and their limitations) are constantly questioned.

One of the most important reasons for the decrease of trust in these norms is that copyright law is viewed, defined, exercised, enforced etc. in the digital age mostly the same way as in the analogue age. A notable illustration for this is connected to the concept of property and ownership (notions that used to be the least fictional legal concepts). Ownership rights generally exist over tangible goods, however, with the advent of electric, electromagnetic and digital technologies, the need to control intangibles has sharply risen. Some countries, like Austria, do accept ownership rights over intangible consumables, like electricity. Assets on a bank account might be owned as well. In copyright law, the same question is painfully problematic. Owning the tangible copy of a work is as ‘natural’ as owning the apple we purchased at the market. But owning a digital file incorporating 0s and 1s that represent a copyrighted expression is far less settled. This conflict is perfectly evidenced by the tensions surrounding the concept of exhaustion (or first sale doctrine in the US legal terminology). Exhaustion allows for the resale of lawfully acquired copies of protected subject matter - as long as the given copy is tangible (Mezei, 2018, pp. 8-10). Exhaustion itself originates from the late 19th century, and it is inherently connected to tangible objects. With the advent of online dissemination methods and channels and the rise of downloadable copies (e.g., iTunes that had a significant role in this respect), the notion of ‘digital exhaustion’ posed a new challenge to this ‘analogue interpretation’ of exhaustion around the beginning of the current Millennium. Many argued that the lawful acquirers of digital copies shall be granted equal ‘rights’ to resell those digital copies to new users (Mezei, 2018; Sganga, 2018). Such a demand has been refused by various court rulings in the European Union and the United States. Such a conclusion might be in line with the words of law, but it completely disregards the ways of digital consumption of media.

A great example for the growing mistrust in copyright law is related to the archetype of accessing contents via the internet, namely, hyperlinking. On the one hand, ‘hyperlinks are the synapses connecting different parts of the world wide web. Without hyperlinks, the web would be like a library without a catalogue: full of information, but with no sure means of finding it’ (Collins, 2010, para. 5.42) On the other hand, in terms of copyright law, hyperlinks allow users to communicate or make available to the public copyright protected subject matter. Hyperlinks are therefore double-edged swords: they are inevitable for a properly functioning internet, but they also help people disobey the existing rules and infringe valuable IP rights. The concurring roles of hyperlinks are fairly reflected by Tim Berners-Lee: ‘Myth: »A normal link is an incitement to copy the linked document in a way which infringes copyright«. This is a serious misunderstanding. The ability to refer to a document (or a person or any thing else) is in general a fundamental right of free speech to the same extent that speech is free. Making the reference with a hypertext link is more efficient but changes nothing else’ (Berners-Lee, 1997, n.p.).

The requirements of lawful linking are still not settled (Mezei, 2016; Quintais, 2018; Frosio, 2020). The many options of musical/audiovisual platforms as well as social networking sites, including embedding functions, autoplay features, sharing possibilities, complicate the question further. Indeed, the European Union’s recent copyright reform (namely, Directive 2019/790 on Copyright in the Digital Single

Market - the CDSM Directive) intended to settle the boundaries of commercial linking activities (while missing to touch upon non-commercial or "private" linking by end users, and hence accepting the permissive approach of Court of Justice of European Union). Article 15 (originally known as Article 11) is, however, coined as "linking tax". This term perfectly reflects society's negative attitude towards any plan to regulate the normal flow of information over the internet. More importantly, Article 15 itself deserves criticism due to the mere fact that it was introduced without any clear empirical evidence to its positive effects. Indeed, recent research indicated that (free) link aggregation is beneficial for the linked site (Roos et al., 2020). Even more worrying, due to the conflicting rulings regarding embedding of images posted on social media platforms, service providers (at least Instagram and Facebook) plan to amend their API terms and conditions to allow users to exclude the 'embeddability' of their posts by other users (Lee, 2020). Such private ordering mechanisms would render linking (and the many supportive court rulings) meaningless - and once again destroy trust in the system.

Another - and maybe the best - example for the significant gap between legal and social norms as well as trust in copyright law is related to P2P file-sharing. Due to various technological developments at the end of the 1990s (e.g., the standardisation of MP3 conversion and the growing internet bandwidth), peer-to-peer exchange of digital files turned out to be the social default for (hundreds of) millions of internet users globally. Although the excess of negative effects of P2P file-sharing on the copyright holders income is questionable, the negative effects themselves are unquestionable (Danaher and Waldfogel, 2012). The copyright industry (especially the American one), however, reacted with an 'analogue mind' to these problems; and intended to destroy the P2P ecosystem (compared to e.g., the Napster [1] and Grokster [2] rulings), which led to the exact opposite result. The reaction of end users was similarly the opposite as expected. Major labels and publishers were not treated to be 'rights holders' anymore, but greedy capitalists limiting online freedoms of end users. The excessive rulings against private users that ordered the payments of hundreds of thousands of dollars (e.g., in the Thomas-Rasset [3] or the Tenenbaum [4] cases); the proceedings against 12 year old children (see the Brianna LaHara 'incident') or dead grandmothers only increased the fury of end users, and seriously harmed the legitimacy of copyright law in general, as well as

[1] A&M Technology Inc. et al. v Napster Inc. et al., 239 *F.3d* 1004 (2001).

[2] Metro-Goldwyn-Mayer Studios Inc. et al. v Grokster Ltd. et al., 545 *U.S.* 913 (2005).

[3] Capitol Records Inc. et al. v Jammie Thomas-Rasset, 692 *F.3d* 899 (2012).

[4] Sony BMG Music Entertainment et al. v. Joel Tenenbaum, 660 *F.3d* 487 (2011).

the enforcement tools specifically.

Indeed, current debates surrounding private ordering mechanisms, that is, enforcement by intermediaries, especially automated law enforcement, lead to concerns related to the use of fundamental freedoms (e.g., freedom to receive and impart information; artistic freedom) over the internet. Private ordering might be the most effective solution to tackle online infringements, its excess and the exact methods used raise serious concerns, too; that again led to the depreciation of trust in copyright law. As Sebastian Felix Schwemer noted, “[p]rivatized enforcement has generally been associated with a variety of issues related to, for example, the rule of law, legal certainty, accountability, democracy deficit, presumption of innocence, right to due process, and potentially right to privacy and freedom of speech and communication” (Schwemer, 2019, p. 5). A notable plan to regulate platforms’ liability that fit into the concept of “online content sharing service providers” is to be found in Article 17 of the Copyright in the Digital Single Market (CDSM) Directive. It requires the clearance of rights related to those protected subject matter that are uploaded to the platforms’ servers by their users [Article 17(1)]; or, alternatively, in the lack of authorisation, it requires the removal (filtering) of the contested contents [Article 17(4)]. Whether this solution will be successful at all, will be seen in the coming years, after the CDSM Directive is implemented by the member states of the European Union. It is, however, telling to see that society (fueled by many politicians as well), including scholars, fear widespread “censorship” of data online (Senftleben, 2020).

Papers

In ‘*Expanding the debate about content moderation*’ (Gillespie et al., 2020), a group of researchers develop their arguments in the form of a roundtable essay. As highlighted by Tarleton Gillespie and Patricia Aufderheide in the introduction, researchers of content moderation have traditionally focussed on high-profile incidents, as for instance related to US presidential elections, pornography or hate speech; and/or on US based (but global leader) platforms, for example Facebook or YouTube (see e.g., Jacques et al., 2018). Content moderation is, however, a much broader and deeper concept, and, in reality, it affects all jurisdictions, more than the biggest platforms, and the topics involved are similarly more complex and expansive. This essay offers a great variety of short contributions by Patricia Aufderheide, Elinor Carmi, Ysabel Gerrard, Tarleton Gillespie, Robert Gorwa, Ariadna Matamoros-Fernández, Sarah T. Roberts, Aram Sinnreich, and Sarah Myers West, ranging from concerns over encryption (a topic further discussed by Heemsbergen and Molnar, 2020 in this special issue); the challenges of regulating social media start-ups; the collaboration of platforms regarding content moderation (or "content cartels"); the alleged neutrality of content moderation; algorithmic content moderation and the risk of false positives and negatives; the regulatory politics of content moderation or the political consequences of commercial content moderation. The editors agree with the conclusion of the authors: "We need more thorough study of the impact of content moderation on different geographical, political and cultural communities" (Gillespie et al., 2020).

One of the most natural reactions of internet users to the challenges posed by massive online surveillance, concerns of privacy and protection of (personal) data over the internet was the general use of encryption services. Measures that intended to strengthen the trust in online solutions cover for instance virtual private networks (VPNs), switching to Hypertext Transfer Protocol Secure (HTTPS) and voluntary data management terms and conditions of online service providers. Luke Heemsbergen and Adam Molnar's contribution to this special issue, titled '*VPNs as boundary objects of the internet: (Mis)trust in the translation(s)*' provides for a look into how one of the technological solutions to secure internet use is understood by Australians, and how VPN service providers construct their products and their governance. Heemsbergen and Molnar's paper combines existing literature on boundary objects and internet studies in an empirical way and addresses the political and legal implications of freedoms and controls over how users encounter and acquire VPN services, how VPN service providers represent and develop their services, and how ultimately regulators reflect these social realities. On of the most telling findings of the paper regarding trust in the system is a quote from a site that reviewed VPN services: "[i]t is important to keep in mind that when you are using a VPN, you are effectively transferring trust from your ISP to the VPN provider" (Heemsbergen and Molnar, 2020).

The paper '*Combating misinformation online: re-imagining social media for policy-making*' (Kyza et al., 2020) is part of the interdisciplinary research project "Co-Creating Misinformation-Resilient Societies", meant to develop online tools and policies to support the civil society and professionals in mitigating the threat of misinformation on social media. The authors, Eleni Kyza, Christiana Varda, Dionysis Panos, Melina Karageorgiou, Nadya Komendantova, Serena Coppolino Perfumi, Syed Iftikhar Husain Shah and Akram Sadat Hosseini, collected data from 67 participants (citizens, journalists, and policymakers) based in Austria, Greece and Sweden, in order to find answers to questions such as *what do real-world policy makers identify as challenges to combating misinformation on social media?* and *which plat-*

form policies are suggested to create a more misinformation-resilient environment on social media? Their analysis resulted in the identification of four important themes, having implications for platform policies and contemporary policymaking: creating a trusted network of experts and collaborators; facilitating the validation of online information; providing access to visualisations of data at different levels of granularity, and increasing the transparency and explainability of flagged misinformative content.

Platforms and platformisation, especially in the videogame industry, have always been in the frontline of technological progress. In '*Playing with platforms: game-making under platform governance*' (Chia et al., 2020), the authors - Aleena Chia, Brendan Keogh, Dale Leorke and Benjamin Nicoll - examine this phenomenon through the lens of two platforms: Unity and Twine, which have transformed videogame creation and distribution. Platformisation is neither a singular, monopolising, or technologically deterministic 'logic' of cultural production, nor a 'one-size-fits-all' concept for describing current technological transformations in the production, distribution, and consumption of media content. On the contrary, the paper argues that videogame development is undergirded by a plurality of platforms and platformisation techniques, some of which counter the top-down vision of platformisation to envision an alternative politics of game-making from the ground-up. The authors have chosen the videogame industry as a key site for analysing the effects of platforms and platformisation on cultural production. Since the mid-2000s, an explosion of different game-making tools, practices, and communities have challenged the conventional formulas of the blockbuster or 'triple A' industry. Today, videogame development is just as, if not more, likely to be conducted by a team of a few precarious independent workers as it is by hundreds of full-time employees in a campus-sized studio. The paper provides an ample definition of key terms such as 'platform' and 'platformisation' in order to outline conceptual blindspots in the scholarly discussion and deployment of these terms, and suggest how critiques of game-making tools can help illuminate these blindspots. Through the case studies, the authors convincingly illustrate how the narratives of platform capitalism and imperialism do not manifest uniformly and could not be assimilated to an all-encompassing conception of either platforms or platformisation.

Next we have Simon Copland's paper '*Reddit quarantined: can changing platform affordances reduce hateful material online?*' (Copland, 2020), which proposes an analytical reflection on the question: how can a digital platform known as a bastion of free speech, one of the last giants to resist homogeneity (which comes with the inherent price of having to “stomach” the occasional troll reddit, in the words of Erik Martin, former Reddit CEO) respond to the increasing pressure to regulate abusive language and online behaviour? Reddit was imagined as a place for open and honest conversations; however, these days, the ‘trolls’ seem to be winning. According to the ranking service Alexa, in 2020, Reddit occupies the 6th place among US sites (with Google, Youtube and Amazon as the top three). Ever since 2012 (with a total revamp in 2018), Reddit has slowly changed its ‘anything goes’ policy, implementing a unique approach - the quarantine function. Quarantined users of the platform cannot generate revenue, and their content does not appear on the front page, nor can be found via search. The function does not ban the content altogether, but simply discourages the spread of abusive material and encourages positive behaviour change. Copland’s paper seizes the opportunity to examine the efficacy of the use of platform bans in limiting hateful content. The author uses two case studies (r/TheRedPill and r/Braincells), data analysis and misogynistic language analysis in order to conclude that the quarantine has mixed results: Reddit indeed saw a drop in hateful activity, but the content and its creators were simply pushed away towards less restrictive (and, therefore, more dangerous) platforms, making it someone else’s problem.

Finally, Maxigas and Guillaume Latzko-Toth discuss how commons were replaced by platforms, or, as the authors state it, “digital interactive media based on open protocols and free software got superseded by proprietary applications embedded within platforms” (Maxigas & Latzko-Toth, 2020). Based on desktop research, data collection and interviews, the paper ‘*Trusted Commons: why ‘old’ social media matter*’ convincingly evidences, how IRC (Internet Relay Chat) survived the emergence of capital-driven platforms, and how it became an example of resistance or recuperation against these platforms these days. Based on the multidisciplinary analysis of free software projects, hackerspaces and Anonymous hacktivists’ political movement, Maxigas and Latzko-Toth show that the “oldness” of IRC is indeed the source of its users’ trust in this protocol, and will indeed survive proprietary platforms, too.

ACKNOWLEDGEMENTS

We would like to thank Frédéric Dubois and the entire *Internet Policy Review* team for their tremendous help and support in publishing this special issue. We especially thank the international peer-reviewers for their deep and thorough support to develop the selected papers: Raluca Bercea, Dan-Adrian Cărămidariu, Glen Fuller, Klára Gellén, István Harkai, Aphra Kerr, Katja Lindroos, Norbert

Merkovity, Gábor Polyák, João Pedro Quintais, Jonathan Roberge, Nicoleta Rodica Dominte and Yoonmo Sang. We would like to wish all the best for the organising committee as well as all participants of the forthcoming AoIR 2020 conference. We are looking forward to reading the fourth special issue of *Internet Policy Review* including excellent AoIR papers in 2021.

References

Association of Internet Researchers. (2019). *#AoIR2019 Call for Proposals*. Association of Internet Researchers. https://aoir.org/aoir2019/aoir2019cfp/

Barlow, J. P. (1996, February). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bauer, J. M., & Eeten, M. J. G. (2009). Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options. *Telecommunications Policy*, *33*(10–11). https://doi.org/10.1016/j.telpol.2009.09.001

Bauman, Z. (2000). *Liquid Modernity*. Polity.

Berners-Lee, T. (1997). *Axioms of Web Architecture—Links and Law: Myths*. W3, Design Issues. http://www.w3.org/DesignIssues/LinkMyths.html

Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*. https://doi.org/10.1177/1461444820939922

Brecht, B. (1979). Radio as a Means of Communication: A Talk on the Function of Radio (S. Hood, Trans.). *Screen*, *20*(3–4), 24–28. https://doi.org/10.1093/screen/20.3-4.24

Brevini, B., Hintz, A., & McCurdy, P. (2013). *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*. Palgrave Macmillan. https://doi.org/10.1057/9781137275745

Bukowski, C. (2001). *Notes of a Dirty Old Man*. City Lights Books.

Burgess, J., & Green, J. (2018). *YouTube: Online Video and Participatory Culture* (Second). Polity Press.

Chang, F. R. (2012). Guest Editor's Column. *The Next Wave*, *19*(4). https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-19-4.pdf

Chia, A., Leorke, D., Keogh, B., & Nicoll, B. (2020). Platformisation in game development. *Internet Policy Review*, *9*(4).

Collins, M. (2010). *The Law of Defamation and the Internet* (3rd ed.). Oxford University Press.

Consalvo, M., & Ess, C. (Eds.). (2011). *The Handbook of Internet Studies*. Wiley-Blackwell. https://doi.org/10.1002/9781444314861

Copland, S. (2020). Reddit quarantined: Can changing platform affordances reduce hateful material online? *Internet Policy Review*, *9*(4).

Danaher, B., & Waldfogel, J. (2012). *Reel Piracy: The Effect of Online Film Piracy on International Box Office Sales*. Social Science Research Network. https://doi.org/10.2139/ssrn.1986299

Del Mar, M., & Twining, W. (Eds.). (2015). *Legal Fictions in Theory and Practice*. Springer. https://doi.org/10.1007/978-3-319-09232-4

Di Salvo, P. (2020). *Digital Whistleblowing Platforms in Journalism. Encrypting Leaks*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-38505-7

Dijck, J., & Rieder, B. (2019). The recursivity of internet governance research. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1418

Dutton, W. H. (2018). Networked publics: Multi-disciplinary perspectives on big policy issues. *Internet Policy Review*, *7*(2). https://doi.org/10.14763/2018.2.795

Elliot, D., & Culver, C. (1992). Defining and analyzing journalistic deception. *Journal of Mass Media Ethics*, *7*(2), 69–74. https://doi.org/10.1207/s15327728jmme0702_1

Elliston, F. (1985). *Whistleblowing: Managing Dissent in the Workplace*. Praeger Publishers.

Ellsberg, D. (2002). *Secrets: A Memoir of Vietnam and the Pentagon papers*. Penguin Books.

Frosio, G. (2020). It’s all linked: How communication to the public affects internet architecture. *Computer Law & Security Review*, *37*. https://doi.org/10.1016/j.clsr.2020.105410

Fuller, L. L. (1930). Legal Fictions. *Illinois Law Review*, *25*(4).

Fuller, L. L. (1967). *Legal Fictions*. Stanford University Press.

Gabielkov, M., Ramachandran, A., Chaintreau, A., & Legout, A. (2016). Social Clicks: What and Who Gets Read on Twitter? *ACM SIGMETRICS Performance Evaluation Review*, *44*(1). https://doi.org/10.1145/2964791.2901462

Gessen, M. (2019). The Difference between Leaking and Whistle-blowing in the Trump White House. *The New Yorker*. https://www.newyorker.com/news/our-columnists/the-difference-between-leaking-and-whistle-blowing-in-the-trump-white-house

Gill, L. (2018). Law, Metaphor, and the Encrypted Machine. *Osgoode Hall Law Journal*, *55*(2). https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/3/

Gillespie, T., Auderheide, P., Carmi, E., Gerrard, Y., Gorwa, R., Matamoros-Fernández, R., T., S., Sinnreich, A., & Myers West, S. (2020). Expanding the debate about content moderation: Scholarly research agendas for the coming policy debates. *Internet Policy Review*, *9*(4).

Gross, P. (2017). Fake news and the digital media. The changing battle for people’s hearts, minds and illusions. *Studia Universitatis Babes-Bolyai - Ephemerides*, *1*, 23–36. https://doi.org/10.24193/subbeph.2017.1.02

Hart, W. (2009). Feeling validated versus being correct: A meta-analysis of selective exposure to information. *Psychological Bulletin*, *135*(4), 555–588. https://doi.org/10.1037/a0015701

Heemsbergen, L., & Molnar, A. (2020). VPNs as Boundary objects of the internet: (Mis)trust in the translation(s. *Internet Policy Review*, *9*(4).

Heldt, A. (2020, June 4). The President and free speech: Consequences of Twitter’s fact-checking indication [[Op-Ed]]. *Internet Policy Review*. https://policyreview.info/articles/news/president-and-free-speech-consequences-twitters-fact-checking-indication/1483

Horn, E. (2011). Logics of Political Secrecy. *Theory, Culture & Society*, *28*(7–8), 103–122. https://doi.org/10.1177/0263276411424583

Hwang, T., & Levy, K. (2015). 'The Cloud' and Other Dangerous Metaphors—Contemporary ideas about data and privacy are tied up inextricably with language choices. *The Atlantic*.

Jacques, S., Garstka, K., Hviid, M., & Street, J. (2018). An Empirical Study of the Use of Automated Anti-Piracy Systems and Their Consequences for Cultural Diversity. *SCRIPTed*, *15*(2). https://doi.org/10.2966/scrip.150218.277

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, *80*(5). https://doi.org/10.1016/j.jcss.2014.02.005

Johnson, R. A. (2003). *Whistleblowing: When it works—And why*. L. Rienner Publishers.

Kitty, A. (2005). *Don't Believe It! How Lies Become News*. The Disinformation Company Ltd.

Klapper, J. (1960). *The Effects of Mass Communication*. The Free Press.

Kyza, E. A., Varda, C., Panos, D., Karageorgiou, M., Komendantova, N., Perfumi, S. C., Shah, S., & Hosseini, A. S. (2020). Combating misinformation online: Re-imagining social media for policy-making. *Internet Policy Review*, *9*(4).

Lakoff, G., & Johnson, M. (2003). *Metaphors We Live By* (2nd ed.). University of Chicago Press.

Larsson, S. (2011). *Metaphors and Norms: Understanding Copyright Law in a Digital Society*. Lund University Press. http://lupak.srv.lu.se/Bokprojekt/visaBok.asp?isbn=91-7267-335-4

Larsson, S. (2017). *Conceptions in the Code—How Metaphors Explain Legal Challenges in Digital Times*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190650384.001.0001

Lee, T. B. (2020). Instagram just threw users of its embedding API under the bus. *Ars Technica*. https://arstechnica.com/tech-policy/2020/06/instagram-just-threw-users-of-its-embedding-api-under-the-bus/

Lessig, L. (2008). *Remix: Making Art and Commerce Thrive in the Hybrid Economy*. Penguin Press.

Marantz, A. (2019, September 30). The Dark Side of Techno-utopianism. *The New Yorker*. https://www.newyorker.com/magazine/2019/09/30/the-dark-side-of-techno-utopianism

Marcus, J. (2017, July 6). The Ethics of Leaks. *NiemanReports*. https://niemanreports.org/articles/the-ethics-of-leaks/)

Maxigas, & Latzko-Toth, G. (2020). Trusted commons: Why 'old' social media matter. *Internet Policy Review*, *9*(4).

Melzer, N. (2019). *Mandate of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment*. United Nations, Office of the High Commissioner for Human Rights. https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24926

Mezei, P. (2016). Enter the matrix: The effects of CJEU case law on linking and streaming technologies. *Journal of Intellectual Property Law & Practice*, *11*(10). https://doi.org/10.1093/jiplp/jpw131

Mezei, P. (2018). *Copyright Exhaustion—Law and Policy in the United States and the European Union*. Cambridge University Press. https://doi.org/10.1017/9781108135290

Milton, J. (1918). *Areopagitica* (R. C. Jebb, Ed.). Cambridge University Press. https://oll.libertyfund.org/titles/103

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, *3*(3–4). https://doi.org/10.1016/j.ijcip.2010.10.002

Mueller, T. (2019). *Crisis of Conscience: Whistleblowing in an Age of Fraud*. Riverhead Books.

Newton, C. (2020, May 29). Why Twitter labeled Trump's tweets as misleading and Facebook didn't. *The Verge*. https://www.theverge.com/interface/2020/5/29/21273370/trump-twitter-executive-order-misleading-facebook-authoritarianism

Nietzsche, F. (1996). *Human, All Too Human: A Book for Free Spirits* (R. J. Hollingdale, Trans.; 2nd ed.). Cambridge University Press.

Palczewski, M. (2017). Fake news. A continuation or rejection of the traditional news paradigm? *Acta Universitatis Lodziensis. Folia Litteraria Polonica*, *43*, 23–34.

Petersen, J. C., & Farrell, D. (1986). *Whistleblowing: Ethical and legal issues in expressing dissent*. Kendall/Hunt.

Quinn, A. (2018). *Virtue Ethics and Professional Journalism*. Springer International Publishing. https://doi.org/10.1007/978-3-030-01428-5

Quintais, J. P. (2018). Untangling the hyperlinking web: In search of the online right of communication to the public. *The Journal of World Intellectual Property*, *21*. https://doi.org/10.1111/jwip.12107

Rochlin, N. (2017). Fake news. Belief in post-truth. *Library Hi Tech*, *35*(3), 386–393. https://doi.org/10.1108/LHT-03-2017-0062

Sagar, R. (2013). *Secrets and Leaks: The Dilemma of State Secrecy*. Princeton University Press. https://doi.org/10.23943/princeton/9780691168180.001.0001

Sang, Y., Lee, J. Y., Park, S., Fisher, C., & Fuller, G. (2020). Signalling and Expressive Interaction: Online News Users' Different Modes of Interaction on Digital Platforms. *Digital Journalism*. https://doi.org/10.1080/21670811.2020.1743194

Schultze, Q. J., & Bytwerk, R. (2012). Plausible Quotations and Reverse Credibility in Online Vernacular Communities. *ETC: A Review of General Semantics*, *69*(2), 216–234. https://www.jstor.org/stable/42579187

Schwemer, S. F. (2019). Trusted notifiers and the privatization of online enforcement. *Computer Law & Security Review*, *35*(6), 105339. https://doi.org/10.1016/j.clsr.2019.105339

Senftleben, M. (2020). The Original Sin—Content 'Moderation' (Censorship) in the EU. *GRUR International*, *69*(4). https://doi.org/10.1093/grurint/ikaa25

Sganga, C. (2018). A Plea for Digital Exhaustion in EU Copyright Law. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, *9*(3).

Stephens, M. (2007). *A History of news*. Oxford University Press.

Thorsen, E., Sreedharan, C., & S, A. (2013). *Wikileaks and Whistle-Blowing: The Framing of Bradley Manning.*(Benedetta Brevini, A. Hintz, & P. McCurdy, Eds.; pp. 101–122). Palgrave Macmillan. https://doi.org/10.1057/9781137275745_7

Thüsing, G., & Forst, G. (Eds.). (2016). *Whistleblowing: A comparative study*. Springer. https://doi.org/10.1007/978-3-319-25577-4

Wardle, C. (2017). Fake News. It's Complicated. [Blog post]. *First Draft*. https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79

Worth, M. (2013). *Whistleblowing in Europe. Legal Protections for Whistleblowers in the EU*. [Report]. Transparency International. https://images.transparencycdn.org/images/2013_WhistleblowingInEurope_EN.pdf

Worth, M. (2015). *Whistleblower protection in Southeast Europe: An overview of laws, practice and recent initiatives*[Report]. Blueprint for Free Speech; Regional Anti-Corruption Initiative. http://rai-see.org/wp-content/uploads/2015/07/Whistleblower_Protection_in_SEE.pdf)

Wyatt, S. (2004). Danger! Metaphors at Work in Economics, Geophysiology, and the Internet. *Science, Technology, & Human Values*, *29*(2). https://doi.org/10.1177/0162243903261947

Zimdars, M. (2016). *False, misleading, clickbait-y, and/or satirical 'news' sources*. https://d279m997dpfwgl.cloudfront.net/wp/2016/11/Resource-False-Misleading-Clickbait-y-and-Satirical-%E2%80%9CNews%E2%80%9D-Sources-1.pdf

Cases

A&M Records, Inc. V. Napster, Inc., 239 F.3d 1004 (United States Court of Appeals for the Ninth Circuit 12 February 2001).

Capitol Records, Inc. V. Thomas-Rasset, 692 F.3d 899 (United States Court of Appeals for the eighth circuit 11 September 2012).

Metro-Goldwyn-Mayer Studios, Inc., et al. V. Grokster, Ltd., et al., 545 U.S. 913 (Supreme Court of the United States 27 June 2005).

Sony BMG Music Entertainment, et al., v. Joel Tenenbaum, 660 F.3d 487 (United States Court of Appeals for the first circuit 16 September 2011).

Published by

Alexander von Humboldt
Institute for Internet
and Society

in cooperation with

CREATe

centre internet et société

UOC R&I IN3 Internet interdisciplinary Institute
Universitat Oberta de Catalunya