6 | 2019
20th Year
15 December 2019
P. 161–192

CRi

Computer Law Review International

A Journal of Information Law and Technology

cr-international.com

Editorial Board: Prof. Dr. Thomas Dreier, M.C.J. · Dr. Jens-L. Gaster · RA Thomas Heymann · Prof. Dr. Michael Lehmann, Dipl.-Kfm. · Prof. Raymond T. Nimmer† · Attorney at Law Holly K. Towle, J.D. · Attorney at Law Thomas Vinje

With Index 2018/2019

Articles ›

Tobias Rothkegel / Laurenz Strassemeyer – Joint Control in European Data Protection Law – How to make Sense of the CJEU's Holy Trinity 161

J. Alexander Lawrence / Kristina Ehle – Combatting Unauthorized Webscraping 171

Ulrike Elteste – Recent Developments in the Law on Payment Services 174

Case Law ›

Canada: Website-Blocking Order Against Innocent ISPs (Federal Court, decision of 15 November 2019 – Bell Media Inc. v. John Doe 1 dba GOLDTV.BIZ) 181

EU: Scope of Host Provider's Duty to Remove Unlawful Information After Court Order (CJEU (3rd Chamber), decision of 3 October 2019 – C-18/18 – Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.) 186

Updates ›

China: The 2019 Draft Measures on Security Assessment of Cross-Border Transfer of Personal Information 189

ottoschmidt

ottoschmidt

86203501906

Exemplar für Lawrence/Ehle

Such scenarios might have to be evaluated differently when Party B will use the results of the rendered analysis also for its own purposes, respectively benefit in the future, provided that both parties at least implicitly accept each other's purposes.[119]

– Party A develops and provides a processing tool/technique to Party B enabling the latter to process its personal data for specific purposes (either carried out by Party B itself or by Party A on behalf of Party B). By providing that tool/technique, Party A – on an abstract level – influences the purposes and means of the processing by Party B.

The deciding factor in this scenario is whether the specific processing directly provides a benefit for Party A. If this is not the case, Party A is either in no capacity involved in the processing (Party B renders the processing by itself) or is merely acting as processor (Party A processes data on behalf of Party B).[120] Insofar, the parties do not jointly determine the purposes of the processing as Party A will solely receive a monetary compensation.

In case Party A will however benefit from the processing carried out by Party B (e.g. by receiving information or results from that processing for its own interests and similar purposes), a joint controllership is rather likely (cf. at para. 47 above).

IV. Overall Conclusion

56 Determining whether joint controllership exists between two or more parties (somehow) involved in the processing of personal data remains highly case-dependent. Insofar, as also underlined by CJEU, all relevant factors of an individual case at hand must be assessed and evaluated in a holistic approach. In this regard, the phase model applied by the CJEU should however lead to rather plausible results as it segregates processing sequences into single processing stages and therein takes into account each party's individual contribution.[121]

57 Nevertheless, certain key criteria can be extracted from the CJEU's judgments that as a rule must be cumulatively met in order to establish a joint controllership between the involved parties. This in turn allows the formation of certain model scenarios and variables that should facilitate an expedient evaluation of potential joint controllership constellations in practice. However, these scenarios may only serve as a starting point for an in-depth assessment of each individual case.

Dr. Tobias Rothkegel

Senior Associate, Osborne Clarke, Hamburg

IT-Law and Data Protection

tobias.rothkegel@osborneclarke.com

osborneclarke.com

Laurenz Strassemeyer

Legal Trainee, Osborne Clarke, Hamburg, and Doctoral candidate at Rheinische Friedrich-Wilhelms-Universität Bonn

IT-Law and Data Protection

laurenz.strassemeyer@osborneclarke.com

osborneclarke.com

119 Cf. *Article 29 Working Party*, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010), p. 19 and 30; *Data Protection Conference*, *Germany (DSK)*, 'Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO' (19 March 2019), p. 3 seq.

120 See also *EDPS*, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (7 November 2019), p. 16.

121 See also *Globocnik*, 'On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID' 2019 IIC, p. 1033, 1036, who later criticises the model, however, from the point of view of the protection of the data subjects; similar *Engeler* and *Marosi*, 'Planet49: Neues vom EuGH zu Cookies, Tracking und ePrivacy' CR 2019, 707, 711 et seq.; for fundamental criticism of the stage model, due to incompatibility with the law system of GDPR, see *Mahieu* and *van Hoboken* 'Fashion-ID: Introducing a phase-oriented approach to data protection?' (30 September 2019), available at: https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/.

J. Alexander Lawrence / Kristina Ehle

Combatting Unauthorized Webscraping

The remaining options in the United States for owners of public websites despite the recent hiQ Labs v. LinkedIn decision

Popular social media websites host a wealth of publicly available information about millions of individuals around the world. The data presents a tempting target for companies that would like to use bots to collect the data without authorization and provide analytic and other services to their own customers. While U.S. law does not yet provide a clear path for individuals to protect their individual interests in such publicly available information, website owners can – and often do – take steps to combat unauthorized webscraping of data from their websites. This typically involves the website owner bringing a civil action against the unauthorized webscraper and seeking a court imposed injunction against such conduct. A recent decision from

ottoschmidt

Exemplar für Lawrence/Ehle

the Ninth Circuit Court of Appeals in a dispute between LinkedIn and hiQ Labs has spotlighted the thorny legal issues involved in combatting unauthorized webscraping of data from public websites. While some may interpret the LinkedIn decision as greenlighting such activity, this would be a mistake. On close review of the decision, and in light of other decisions that have held unauthorized webscrapers liable, the conduct remains vulnerable to legal challenge in the United States.

I. Background

1 Founded in 2012, hiQ Labs, Inc. (hiQ) is a data analytics company that uses automated bots to scrape information from LinkedIn's website. hiQ targets the information that users have made public for all to see in their LinkedIn profile. hiQ pays nothing to LinkedIn for the data, which it uses, along with its own predictive algorithm, to yield "people analytics", which it then sells to its clients.

2 In May 2017, LinkedIn sent a cease-and-desist letter to hiQ demanding that it stop accessing and copying data from LinkedIn's servers. LinkedIn also implemented technical measures to prevent hiQ from accessing the website, which hiQ circumvented.

1. hiQ's Injunctive Relief

3 Shortly thereafter, with its entire business model under threat, hiQ filed suit in the United States District Court for the Northern District of California seeking injunctive relief and a declaration that LinkedIn had no right to prevent it from accessing public LinkedIn member profiles and copying data from them.

4 Without access to LinkedIn public member profile data, hiQ argued that it would likely be forced to breach its existing contracts with clients and to pass up pending deals with prospective clients. hiQ further noted that it was in the middle of a financing round when it received LinkedIn's cease-and-desist letter and that in light of the uncertainty about the company's future viability, that financing round stalled. hiQ claimed that if LinkedIn prevailed, it would have to lay off most, if not all, of its employees and shutter its operations.

5 In August 2017, the district court granted hiQ's motion for a preliminary injunction. It ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing technical barriers to hiQ's access to public member profiles, and to refrain from putting in place any legal or technical measures with the effect of blocking hiQ's access to public member profiles.

2. LinkedIn's Appeal

6 As is the case with preliminary injunction orders, the district court did not reach a final decision on the merits. Rather, the district court's preliminary injunction order was limited to maintaining the status quo while the case proceeds through the normal process to a final decision on the merits.

7 As authorized under U.S. law, LinkedIn appealed the district court's preliminary injunction order. More than two years passed.

II. Approach by the Ninth Circuit

On 9 September 2019, a three-judge panel of the Ninth Circuit affirmed the district court's preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles. 8

1. Likelihood of Irreparable Harm

The court concluded that the district court did not abuse its discretion in finding that hiQ established a likelihood of irreparable harm because the survival of its business was threatened. The court further held that the district court did not abuse its discretion in balancing the equities and concluding that, even if some LinkedIn members retain some privacy interests in their information notwithstanding their decision to make their profiles public, those interests did not outweigh hiQ's interest in continuing its business. 9

2. Tortious Interference with Contract & Legitimate Business Purpose

While not ruling in favour of hiQ on the merits, the court held that the district court did not abuse its discretion in finding that hiQ raised serious questions not only going to: 10

(1) the merits of its claim for tortious interference with contract, alleging that LinkedIn intentionally interfered with hiQ's customer contracts, but also

(2) the merits of LinkedIn's legitimate business purpose defence to hiQ's tortious interference claim.

3. CFAA Defence

hiQ also raised a serious question as to whether its state law causes of action for tortious interference and unfair competition were preempted by the Computer Fraud and Abuse Act (CFAA), as LinkedIn alleged as its principal defence. The CFAA prohibits intentionally accessing a computer[1] without authorization, or exceeding authorized access, and thereby obtaining information from any protected computer. In particular, the court concluded that hiQ had raised a serious question as to whether the CFAA's reference to access "without authorization" limits the scope of statutory coverage to computer information for which authorization or access permission, such as password authentication, is generally required. 11

4. Limited Impact

In short, the court held that the district court did not abuse its discretion in finding that hiQ had made a sufficient showing under the preliminary injunction standard to obtain an order 12

1 The term "computer" is broadly defined in the CFAA. *See* 18 U.S.C. § 1030(e)(1) ("the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.").

ottoschmidt

Exemplar für Lawrence/Ehle

allowing it to continue to operate its business until the merits of the case were decided.

13 Notably, the court recognized that at the preliminary injunction stage, it was not resolving the companies' legal dispute definitively, nor was it addressing all the claims and defences they had pleaded in the district court. The court noted that it was considering only the claims and defences that the parties pressed on appeal and for which the companies had invoked additional claims and defences in the district court. The court expressed no opinion as to whether any of those other claims or defences might ultimately prove meritorious.

14 In particular, the court recognized that while LinkedIn asserted that it has "claims under the Digital Millennium Copyright Act and under trespass and misappropriation doctrines," it chose for purposes of the appeal to focus on the CFAA defence, such that this was the sole defence to hiQ's claims that the court addressed on appeal.[2]

III. Comments and Practical Implications

15 Prohibitions on webscraping can take many forms, and liability for unauthorized webscraping can be imposed under numerous legal theories under U.S. law. That one of those legal theories failed at the preliminary injunction stage in LinkedIn's case does not mean it will fail in most cases.

1. Diverging Legal Opinions on Application of the CFAA

16 While the Ninth Circuit panel took a narrow view of the scope of the CFAA, not all courts would agree with that view. For instance, in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003), the First Circuit Court of Appeals, which hears cases from federal district courts in Maine, New Hampshire, and Massachusetts, considered a case in which the plaintiff, who operated a travel website, brought suit against a competitor that used webscrapers to obtain pricing information from the plaintiff's public website. The First Circuit held that the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers [and that a] public website provider can easily spell out explicitly what is forbidden" and if it "wants to ban scrapers," it may do so. The First Circuit held that a "lack of authorization could be established by an explicit statement on the website restricting access."[3] Thus, even with publicly available data, like that on LinkedIn's site, some courts have held that accessing a website after being expressly informed that further access is unauthorized can violate the CFAA.

2. Security Threshold for Data Access

17 Moreover, the Ninth Circuit panel recognized that websites that place greater protections on their data may still be able to make out a claim under the CFAA. Notably, the decision does not overturn a prior panel decision regarding unauthorized access to Facebook data.[4] In that case, the party accused by Facebook of unauthorized access to the data had authorization from Facebook users, but not Facebook. Facebook sent a cease-and-desist letter to the company informing it that further access was unauthorized. This panel distinguished the prior panel decision with respect to Facebook data on the basis that the LinkedIn data is not protected by a username and password authentication system, but rather is available to anyone with a web browser.

3. Alternative Legal Claims

18 The Ninth Circuit panel was also careful to note that victims of webscraping are not without resort, even if the CFAA does not apply. The court recognized that alternative claims may also lie including claims for:

2 In its cease and desist letter, LinkedIn asserted rights under the Digital Millennium Copyright Act (17 U.S.C. §§ 512, 1201) ("DMCA"). The DMCA prohibits "circumvent[ing] a technological measure that effectively controls access" to a "work protected under this title." 17 U.S.C. § 1201(a)(1)(A). "[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3) (emphasis added). In its motion for a preliminary injunction, hiQ argued that any measures LinkedIn implemented to block hiQ from accessing members' public profile information on LinkedIn fall outside of the DMCA because such measures are – among other things – not implemented "with the authority of the copyright owner." 17 U.S.C. § 1201(a)(3). Pointing to the LinkedIn user agreement, hiQ noted that any copyrights to LinkedIn user profiles are owned by LinkedIn's users, not LinkedIn. Thus, any technological measure LinkedIn implemented to control access to a user's public profile information was implemented with only the authority of LinkedIn, not the member. Even with respect to the members, there would be serious questions whether the type of data on LinkedIn is protected by the Copyright Act. *See Feist Pub'ns, Inc., v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991) (holding information alone without a minimum of original creativity cannot be protected by copyright). In any event, LinkedIn did not address the DMCA argument in its opposition to the motion for preliminary injunction, and hiQ argued that LinkedIn had abandoned any DMCA arguments asserted in the cease and desist letter. The district court did not address the DMCA claims in its decision, and thus the issue was not before the Ninth Circuit on appeal.

3 Other lower federal district courts are in accord. *See, e.g., Sw. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (holding Southwest Airlines had plausibly alleged the "without authorization" element of its CFAA claim where the complaint contained allegations that it "directly informed" the defendant that its web-crawling activity was prohibited via Southwest.com's Use Agreement, which was "accessible from all pages on the website," as well as via "direct 'repeated warnings and requests to stop scraping.'"); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013) (even though "Craigslist gave the world permission (i.e., 'authorization') to access the public information on its public website," Craigslist "rescinded that permission for 3Taps. Further access by 3Taps after that rescission was 'without authorization.'"); *Couponcabin LLC v. Savings.com, Inc.*, No. 14-CV-39, 2016 WL 3181826, at *3–4 (N.D. Ind. June 8, 2016) ("CFAA liability may exist in certain situations where a party's authorization to access electronic data-including publicly accessible electronic data-has been affirmatively rescinded or revoked"); *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595–97 (E.D. Pa. 2016) (following "CFAA cases" that have concluded that "a web-user acts without 'authorization' when it crawls a public website").

4 *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), cert. denied, 138 S. Ct. 313 (2017).

ottoschmidt

Exemplar für Lawrence/Ehle

– trespass to chattels,[5]
– copyright infringement,
– misappropriation,
– unjust enrichment,
– conversion,
– breach of contract,[6] or
– breach of privacy (depending on the type of data obtained and whether it was publicly available).

IV. Conclusions

19 Thus, the decision should not be interpreted as greenlighting unauthorized webscraping. And it is important to note that no court has yet reached a decision on the merits in the LinkedIn case. The Ninth Circuit panel decision only addresses the district court's preliminary injunction order. LinkedIn has also filed papers expressing its intention to seek review by the United States Supreme Court. Thus, it remains unclear which party will ultimately prevail.

20 However the case turns out, the decision emphasizes the need to act promptly against unauthorized webscrapers. The court clearly gave weight to the allegation that LinkedIn was well aware of hiQ's practices for years before sending the cease-and-desist letter. The court further expressed concern that LinkedIn sent the cease-and-desist letter because it planned to create a new product that competed with hiQ's services, which the court held could raise concerns under California's unfair competition laws. To avoid such claims under U.S. law, unauthorized webscrapers should be addressed promptly before they free ride for years and build a business off your data.

J. Alexander Lawrence

Partner at Morrison & Foerster, Tokyo

Commercial Litigation, Intellectual Property Litigation, Litigation

alawrence@mofo.com

mofo.com

Kristina Ehle

Partner at Morrison & Foerster

Attorney-at-law and Co-Managing Partner of Morrison & Foerster's Berlin office

Technology Transactions, Copyright, Media + Entertainment

kehle@mofo.com mofo.com

5 While LinkedIn did not press the claim on appeal, the Ninth Circuit specifically recognized that webscraping exceeding the scope of the website owner's consent can give rise to a common law tort claim for trespass to chattels. *Compare eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (finding that eBay had established a likelihood of success on its trespass claim against the auction-aggregating site Bidder's Edge because, although eBay's "site is publicly accessible," "eBay's servers are private property, conditional access to which eBay grants the public," and Bidder's Edge had exceeded the scope of any consent, even if it did not cause physical harm); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) (holding that a company that scraped a competitor's website to obtain data for marketing purposes likely committed trespass to chattels because scraping could – although it did not yet – cause physical harm to the plaintiff's computer servers); *Sw. Airlines Co. v. FareChase, Inc.*, 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004) (holding that the use of a scraper to glean flight information was unauthorized as it interfered with Southwest's use and possession of its site, even if the scraping did not cause physical harm or deprivation), *with Ticketmaster Corp. v. Tickets.Com, Inc.*, No. 2:99-cv-07654-HLH-VBK, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (holding that the use of a web crawler to gather information from a public website, without more, is insufficient to fulfill the harm requirement of a trespass action); *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1364 (2003) (holding that "trespass to chattels is not actionable if it does not involve actual or threatened injury" to property and the defendant's actions did not damage or interfere with the operation of the computer systems at issue).

6 The Ninth Circuit noted that while LinkedIn's terms of use specifically prohibited webscraping, hiQ was no longer bound by those terms of use because LinkedIn had terminated its user status. Other courts may not agree that, once clearly informed of the terms of use, the continued violation of the terms would not provide the basis for a breach of contract claim. *See, e.g., Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401 (2d Cir. 2004) (holding Verio's numerous and repeated queries to Register.com's servers were sufficient to show that Verio knew of, and was bound by, Register.com's terms).

Ulrike Elteste

Recent Developments in the Law on Payment Services

Overview of implementation and application of PSD II in Germany between January 2018 and October 2019

The new safety requirements under the Second Payment Services Directive (PSD II) came into effect on 14 September 2019. Their interpretation and the supervisory practice in Germany lead to certain limitations in the scope of their application. German courts dealt with, inter alia, charges for the use of specific payment methods, the allocation of liability in fraud cases, charge-

Exemplar für Lawrence/Ehle