CREATe Working Paper 2013/2 (March 2013)

“CCTV sniffing”: Copyright and Data Protection Implications*

Authors

Smita Kheria
University of Edinburgh
smita.kheria@ed.ac.uk

Daithi Mac Sithigh
University of Edinburgh
Daithi.mac.sithigh@ed.ac.uk

Judith Rauhofer
University of Edinburgh
Judith.rauhofer@ed.ac.uk

Burkhard Schafer
University of Edinburgh
b.schafer@ed.ac.uk

University of Edinburgh, School of Law, SCRIPT Centre, Old College, South Bridge, Edinburgh EH8 9YL, UK

CREATe Working Paper Series DOI: 10.5281/zenodo.8372.

This release was supported by the RCUK funded *Centre for Copyright and New Business Models in the Creative Economy (CREATe)*, AHRC Grant Number AH/K000179/1.

Keywords: ***Warspying, Computer misuse Act, Copyright Law, CCTV sniffing***

Abstract*:* *This paper discusses the legal implications of CCTV sniffing and war walking, legally problematic uses of wireless networks, for the purpose of art. Using Bitnik's "surveillance chess" as starting point, it asks if new forms of computer enabled art require new forms of protection, especially in countries without constitutional guarantee for freedom of art.*

1. Artists on the warpath

1.1. Surveillance Chess

In the spring of 2012, the Zurich based Art collective Bitnik visits London in the process of preparation for the Olympic Games. Here they execute one of their notorious performance hacking/art events, "Surveillance Chess", an example of what is called variously "CCTV sniffing" or "warspying". In one of London's iconic tube stations, they hack into one of the ubiquitous surveillance cameras and (claim to) assume control over its transmission.[1] They replace the real-time surveillance images and send the security staff an invitation to play a game of chess, rendering their control room into a game's console.

The results are two distinct works of art. One, reflecting the understanding of the artists, is a live performance for and with the security staff as audience. They are invited to phone in their chess moves to a mobile number sent to them through the CCTV feed. The other is a video collage that merges actual CCTV footage with images of the chessboard.[2] On this video, we see a group of business people with their suits open making their way to the exit, a man who could lose a few pounds and a young woman looking for way out, or a group of commuters walking to the next connection, one of them, apparently, breaking the law by lighting up a cigarette. Their faces are as the CCTV operators would see them, unpixilated and easily identifiable. At the point in time when Bitnik takes over, the CCTV operator allegedly loses control over their system, from their God-like perspective, all-seeing but remote, they suddenly become blinded but involved. "I am controlling your CCTV camera now. I am the one with the yellow suitcase." The camera feed shows a woman with a yellow suitcase. Then the image switches to the chess board. "How about a game of chess? A disembodied voice asks the security staff. "You are white. I am black. Call me or text me to make your move. This is my number: 07582460851." According to the artists: "The work "Surveillance Chess" shows that it is possible to intervene into surveillance systems in public spaces. It also shows how easy it

* Work on this paper was supported by the RCUK CREATE network grant, www.create.ac.uk. We are also grateful to Raphael Satter, journalist for AP, whose query triggered this paper, and to the discussions with Jane Cornwell. A modified version of this paper was published as (Mis)appropriation Art? : Copyright and Data Protection implications of 'CCTV Sniffing' as Art. / Kheria, Smita; Mac Sithigh, Daithi; Rauhofer, Judith; Schafer, Burkhard. Abstraktion und Applikation. ed. / E Schweighofer; F Kummer; W Hötzendorfer. OCG, 2013. p. 489-98.

[1] While the artists claim on their website that they are indeed capable of taking over the CCTV feed, this claim could not be independently verified. For the purpose of this analysis however, we will assume that they were indeed capable of not receiving the wireless transmission, but to send images directly from their computer to the CCTV controlling station.

[2] http://vimeo.com/46236909

is not only to shift the power structure of these systems, but to reverse them altogether."[3] This paper explores some of the legal issues generated by this form of performance art. Was the creation of the work legal? Is the resulting art copyright protected? In doing so, we will examine some generic issues that the interaction between art and new technologies creates for the law and legal regulation.

Bitnik are no novices to legal controversy in London. In 2010, UBS successfully prevented Bitnik from displaying a 20m advertising poster as part of their "Too Big To Fail/ Too Small To Succeed" exhibition.[4] The poster, which would have been displayed outside the exhibition hall on a commercial billboard shows a man outside the UBS headquarter in Zurich, holding a placard with the words "lies" – at a time when UBS's involvement in the banking crisis was under scrutiny. UBS contacted the commercial agency that owned the billboard and threatened action for trademark violation, on the grounds that the UBS logo was visible on the display. This rather problematic claim was particularly ironic as the picture was indeed based on another person's creative thoughts – it was a reenactment and update of the iconic photograph "The police lies" by the Austrian conceptual artist Peter Weibel from the 1970s. His photo addressed the monopoly of power by the state and its organs, a concern with power structures and their subversion that is also preeminent in the works of Bitnik, but updated for the internet society.

Nor was "Surveillance chess" the first project by Bitnik using technology to challenge and subvert new, ICT enabled power structures. "Hacking" for them are artistic manipulations of a system to change it to something other than its original purpose. Previous events had included guided city walks in Bern, where members of the public identified open wireless networks and marked them on a map.[5] More audacious though was an event that did not rely on wireless networks. "Opera Calling" was an attempt artistically to subvert the commercial and power structure of „big art". Bugs were placed in the stalls of the Zurich Opera, to give a wider audience access to the performance. The audio signal was however not broadcasted via radio or the internet. Instead, every listener received the transmission individually via telephone. More than 90hrs of recording were delivered in this way to over 4000 people.[6]

The common theme of all these events is the use of technology to highlight existing power structures. From a legal perspective, the common theme raises questions of copyright, data protection and network integrity. We will focus on "Surveillance chess" as the most problematic, and technologically and legally challenging, of their performances. However, it is important to keep this wider context in mind when addressing the issue of whether new forms of computer enabled art require a new approach to the question of legal regulation of ICT.

1.2. Sniffing out Art

Bitnik was not the first group to use unsecured wireless CCTV networks for artistic purposes. An earlier, and legally less problematic, example comes from the British artist David Valentine. He uses CCTV cameras the same way a filmmaker would use a camera crew. A passive, listen-only wireless network detector, sniffer, and intrusion detection system such as Kismet[7] is used to identify the location of unsecured wireless CCTV networks. His actors,

[3] http://chess.bitnik.org/about.html
[4] http://www.woz.ch/1039/zensur/der-lange-arm-der-ubs
[5] http://www.haus-ek.org/de/node/164?loc=PVA
[6] http://www.hacking-the-city.org/artists-and-projects/mediengruppe-bitnik.html
[7] http://www.kismetwireless.net/documentation.shtml

often teenagers from disadvantaged backgrounds, then perform in front of the CCTV camera. The transmission of the recording is then intercepted and copied – this way, a "traditional" film is made with the CCTV camera as recording device. According to Valentine:

"I'm now working on a project I've had in mind for a while; a musical, based on West Side Story. I'll be filming in Basildon in Essex, England with 20 actors. I'm basically going to use whatever CCTV cameras I can get my hands on. Primarily, this will come from the town centre and the shopping centre CCTV. But I'm also looking at personal CCTV cameras worn by Basildon police and may include wireless cameras I can sniff in the area as well. [In total] the figure will be in the hundreds! Even though I personally don't like being filmed all the time, my work isn't politically driven. It's rather an attempt to retake control of the environment and allow socially disadvantaged kids to use technology freely and be creative."[8]

While Valentine denies any political motivation, others see the potential for challenging our surveillance culture through art. Typical for this approach is Monika Vykoukal, curator at Peacock Visual Arts:

"A few months ago, we set up an exhibition about new media that focused on surveillance and the way technology affects life. Several CCTV films were screened, including "Faceless" by Manu Luksch and "The Duelists" by David Valentine. I feel that making CCTV films is a way to call video surveillance into question and to trigger a reflection about its use."[9]

It is against this backdrop that Bitnik's choice of pre-Olympic London as stage gains particular potency, and also possibly legal relevance. Britain already has the highest density of CCTV cameras in Europe, with London again leading the league table.[10] As part of the security for the games, this surveillance network increased not just in quantity, but also quality. Examples include for instance the combination of visual CCTV with directed audio-surveillance that permits "listening in" on verbal exchanges between suspects. At the same time, the organizing committee of the 2012 London Games attempted to police the use of portable Wi-Fi hotspots and 3G hubs at Olympic venues.[11] Sniffing software similar to that used by Bitnik was used by officials to identify the source of signals of a frequency not explicitly authorized for use at Olympic sites by the U.K. Office of Communications.[12] While it was claimed that the reason for this was to ensure uninterrupted transmission of necessary signals, it is at least questionable if Wi-Fi with its 2.4GHz band could interfere with transmission typically on the 450MHz and 800MHz wavelength. Instead, the motive could have been protection of trademarks and transmission rights, to enforce the ban by London Olympics that prohibits ticket holders from sharing their own photos and videos on any social media like Facebook.[13]

The obvious relevance of Bitnik's art for both phenomena, and its close association to the games and the city, could trigger public interest defenses against those possible legal infractions that we will analyse in the second part of this paper.

---

[8] The Observers 15/09/2008 http://observers.france24.com/content/20080915-cctv-surveillance-video-artists-sniffing

[9] Ibid.

[10] Schafer, B. 'Schlafwandelnd in den Überwachungsstaat?' (2009) *Datenschutz und Datensicherheit*. 8 483-489

[11] Raphael Satter, Olympic Wi-Fi police on hunt for rogue hotspots, http://www.cbc.ca/news/technology/story/2012/08/02/tech-ioc-Wi-Fi-hotspots-banned.html

[12] http://stakeholders.ofcom.org.uk/binaries/consultations/london2012/statement/statement.pdf

[13] Dan Reyes "Sorry, No Social Sharing at the London Olympics", Technorati May 06, 2012 at http://technorati.com/social-media/article/sorry-no-social-sharing-at-the/

1.3. Where artists roam free

Before we can attempt a legal analysis, some of the underlying technical issues of CCTV sniffing and war-driving need to be discussed. The terminology in this field is generated by the hacking community and often lacks consistency. The basis of Bitnik's or Valentine's actions is an activity known as "CCTV sniffing", a form of interference with open wireless networks that is also often referred to as warsyping, warviewing or warwatching.[14] The concept can be traced back to a talk by Peter Shipley to the hacker community at DEFCON 9 in 2001.[15] At its most basic, warspying is to "sniff" 802.11 traffic with a wireless receiver in monitor mode. In this mode, it receives all traffic, regardless of the intended target. The term "War spying" was formed in analogy to "war dialing" in John Badham's 1983 Cold War thriller WarGames. In the film, the character of David Lightman, a high school student, hacks into the district's computer system to alter his grades, accidentally bringing the world close to a thermonuclear war when the "game" he finds in the process turns out to be a simulation run on the national defence computer system. To get access to the system, he scans entire ranges of phone numbers for the carrier tones that is typical for a modem.

Once he hears the modem's carrier tone, he has found a receptive appliance, and can record a "hit."[16]. Warspying uses the same principle, but applied to wireless networks. There are also more mundane applications of this idea, designed to assist the owner of a WLAN to check signal strength or leakage.

Soon however, warspying was turned by the hacking community into a competitive game. WarViewing became synonymous with the competitive hunt for unprotected 2.4 GHz video feeds that characterize open wireless networks, while for the more mundane applications, "wireless monitoring" is usually used as term. WarViewers typically combine the Wi-FiWi-Fi-equipped device with a GPS device to record the location of the wireless networks that they discover. Websites like WiGLE, **Wi**reless **G**eographic **L**ogging **E**ngine[17] allow them to upload the data and transform it into maps of the network neighborhood. There are also educational uses: in 2004, 100 undergraduates from the Department of Communication at the University of Washington mapped the city of Seattle in this way. 44% of the more than 5000 access points that they found were secured with WEP encryption, 52% were open, and 3% were pay-for-access. Many of the open networks clearly identified themselves as open access, with network names like "Open to share, no porn please" or "Free access, be nice." The information was published online in high-resolution maps.[18] Today, warviewing has become mainstream, with even a Nintendo's *Treasure World* game being based on the idea. Wardriving, WarWalking and similar derivations indicate the method of transport used by the WarViewer. WarChalking finally is the practice to leave physical signs in the vicinity of an open network that one has identified, to facilitate their use by other parties. This custom, based on the "Hobo

[14] Ryan, Patrick S., War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics. Virginia Journal of Law & Technology, Vol. 9, No. 7, Summer 2004

[15] Hal Berghel, Wireless Infidelity I: War Driving. Communications of the ACM, September 2004/Vol. 47, No. 9 p 21-26 at p. 21

[16] Ibid p. 23

[17] http://wigle.net/

[18] Marwick, Alice (15 February 2005). "Seattle Wi-Fi Map Project". *Students of COM300, Fall 2004 - Basic Concepts of New Media*. http://depts.washington.edu/Wi-Fimap/

signs" of the Great Depression creates additional security risks if a malicious user identifies a sign left by a benevolent hunter.[19]

The "sniffing" that underpins WarViewing can be either purely passive, listen-only, or semi-active. The above-mentioned "Kismet" program falls into the first category. In this case, the sniffer does not communicate at all with the networks, an analogy is to hear someone shouting and in this way identifying him. Other software actively sends probe messages to which the access point automatically responds. A typical example is NetStumbler.[20] In this scenario, the warviewer becomes temporarily associated with the network, even though no data is transferred. An analogy would be to shout "is someone there?" and to wait for a response.

For WarViewing, nothing more is necessary. Bitnik's Basel event falls into this category of "pure" WarViewing that only records the location of Wi-fi enabled CCTV. However, the situation changes when the network identified by the warviewer is unencrypted and unsecured. In this case, they can also make use of the network. Bitnik's Surveillance Chess and Valentine's film projects in varying degree fall into this category.

Intentional access of an open Wi-Fi network without harmful intent, free riding on the subscription of the owner of the hotspot has paid but without causing him any damage, is sometimes referred to as "piggybacking" or "wi-fi hijacking".[21] Access with harmful intent by contrast is sometimes referred to as Whacking, a portmanteau of "wireless" and "hacking".[22] Frequently, the specific form of malicious attack on an open Wi-Fi network will be what is called *Warkitting*, a combination of wardriving and rootkitting, where the firmware of an attacked router is replaced by the attacker. This allows them to control all traffic for the victim.[23] In a study from 2006, 10% of the wireless routers were susceptible to WAPjacking (in this case the firmware settings are changed, but the firmware itself is left untouched) and 4.4% of wireless routers were vulnerable to WAPkitting (actually changing the router firmware).

2. All is fair in law and war

With an understanding of the potential of an artistic use of Warviewing established, and with a basic understanding of the relevant techniques and vocabulary, we can now turn to the question of the legal implications of artworks such as Surveillance Chess or Valentine's Duel. We will first discuss the data protection and criminal law implications, before moving on to a discussion of the intellectual property aspects. This is because of the potential implications for the copyright position that come from prior illegal activity in the generation of the work.

---

[19] Lawrence, E.; Lawrence, J.; , "Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking," *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on* , vol.2, no., pp. 268- 273 Vol.2, 5-7 April 2004

[20] http://www.stumbler.net/

[21] See e.g. Griffiths, Peter (2007-04-18). "Two cautioned over wireless "piggy-backing" http://www.reuters.com/article/2007/04/18/us-britain-wireless-idUSL1848090220070418

[22] Benjamin D. Kern, Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101 (2004)

[23] A. Tsow, M. Jakobsson, L. Yang, S. Wetzel. "Warkitting: the Drive-by Subversion of Wireless Home routers ." Journal of Digital Forensics Practice, Vol. 1, No. 3, 2006, pp. 179-192.

2.1. Every work of art is an uncommitted crime

Is it legal for artists to use open, unsecured Wi-Fi networks to create art? The answer, obviously, is "it depends". More specifically, it depends on

- the jurisdiction
- the precise technology that was used
- possibly the resulting work, if a specific privilege or justification is argued.

In the UK, three pieces of legislation in particular might be relevant, the Computer Misuse Act 1990, section 125 of the Communications Act 2003 and as an outside possibility section 1(2) of the Regulation of Investigatory Powers Act 2000 (hereafter RIPA).

A conviction under any of the three provisions requires unauthorized access to be found. Of the methods of warspying discussed above, this means that purely passive, listen-only warspying is not covered by any of them. Potentially questionable is however if even probe messages that result in a temporary association with a network, but no data transfer, qualifies as access. There are no relevant UK cases that settle this question. The US case of *State v. Allen*[24] however could be persuasive. This older case dealt technically speaking with wardialing. Allen had tried to gain access to free long distance calls, but aborted the attempt when asked for a password. The Court distinguished in this case "contacting" or "approaching" a computer system from "accessing" it.[25] If this interpretation is followed in the UK, then Bitnik's Basel tour, a traditional Warspying event, should be legal without regard to the software used to identify the network and the CCTV camera

More problematic is the use of CCTV cameras for the creation of films as in Valentine's projects, as example of piggy-backing. The Computer Misuse Act is not applicable, since no unauthorized changes to the computer system are carried out. The interpretative section 17(2) 3 is also not applicable. While it does not require changes to the computer, Valentine also does not *use data on the* computer, he intercepts it in transmission. The CCTV camera does exactly what it is intended to do – record the activities of people – and the interception of the transmission is purely passive, akin to overhearing someone else talking. However, he now uses a service without authorization. This may make him liable under Section 125 of the Communications Act 2003 which creates a criminal offence for "a person who dishonestly obtains an electronic communications service who does so with intent to avoid payment of a charge applicable to the provision of that service. The paradigmatic case for this provision is clear – manipulating e.g. my telephone line so that calls that I make are not "logged" by the provider. Whether use of open access networks falls under the provision is contested.[26] There is a paucity of cases that clarify the law, on point being e.g. the conviction of Gregory Straszkiewicz in 2005 who was convicted to a £500 fine when local residents complained that he repeatedly tried to gain access to their networks with a laptop from a car.[27] The legal fiction in this case is that he deprives the ISP of the owner of the network router from the fee he would otherwise have paid to gain access to the internet. After initially contradictory decisions by lower courts, German courts now seem to reject this interpretation.[28] In our

[24] State v Allen 260 Kan. 107 (1996)
[25] Bierlein, Matthew (2006). "Policing the Wireless World: Access Liability in the Open Wi-Fi Era". *Ohio State Law Journal* **67** (5).
[26] D M Síthigh, "Law in the Last Mile: Sharing Internet Access Through Wi-Fi", (2009) 6:2 *SCRIPTed* 355, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.asp
[27] Jane Wakefield. Wireless hijacking under scrutiny, http://news.bbc.co.uk/1/hi/technology/4721723.stm
[28] *LG Wuppertal, Beschluss vom 19. Oktober 2010 - 25 Qs-10 Js 1977/08-177/10* in: MIR 2010, Dok. 156

cases, this interpretation would be even more far fetched. Valentine or Bitnik are not even potential customers of the provider of CCTV surveillance providers in the London underground. Indeed, it would be illegal under Data Protection Law for them to monitor third parties in the absence of a legitimate interest.

Unproblematic again, though this time in favour of liability, is undoubtedly *Surveillance Chess*. While the Communications Act 2003 remains irrelevant, here an unauthorized modification of a computer system, a whacking, took place. The Computer Misuse Act applies as a result. That the intent is ultimately benevolent – entertaining the security officer and educating the public - is legally irrelevant. It is also possible that Bitnik violated section 1(2) RIPA. For this, their actions would have to be constructed as intentionally and without lawful authority, […] intercepting communication in the course of its transmission by means of a private telecommunication system. Questionable could be if a CCTV system is a "private communication system" for the purpose of RIPA. It is most certainly not a paradigmatic case – like intercepting emails in a company intranet – not the least because the sender in this case is an automated system. However, when Google got into trouble over the collection of payload data from Wi-Fi networks by its Street View service, the Metropolitan Police did consider a complaint by a privacy organization that this constituted a violation of RIPA[29]. Although it later decided "after consultation with the Information Commissioner's Office" that "it would not be appropriate to launch a criminal investigation"[30], much of this decision was based on Google's claim at the time that the collection of the data was accidental. A German police force closed its investigation in 2012 for similar reasons[31]. There are no precedents of the interception of CCTV footage that would settle the issue, but with the reluctance of UK judges to apply purposive interpretation, and the wording of the statute, a conviction seems at least possible. In this case, we should note that the argument applies just as well to Valentine's example – both are cases of purely passive interception, but interception nonetheless.

In addition to criminal charges under the Computer Misuse Act or RIPA, there is also a question of data protection law. As in the previous section, this is particularly pertinent for *Surveillance Chess*. While there is a possibility that third parties are accidentally filmed in Valentine's projects, the focus of the camera would not be on them and it is unlikely that they would be identifiable.[32] However, as we noticed in the introduction, the unpixilated images of users of the London Underground do indeed focus very clearly on individuals, and show them in sometimes embarrassing poses or situations. This raises two issues – liability of the CCTV provider under the Data Protection Act (hereafter DPA), and liability of Bitnik for storing and subsequently publishing the CCTV footage that they gained hold of. For the former, allowing Bitnik access to the footage amounts to a data security breach, i.e. a breach of the seventh data protection principle. The CCTV owner failed to take the appropriate technical and organisational steps to secure the wireless transmission of the images. This is a requirement that is highlighted in the ICO's 2008 CCTV Code of Practice. However, the artists themselves, when publishing the images of people recorded in a way that allows identification might also be found in breach of the DPA although they will most likely try to rely on the "journalistic, literary or artistic purposes" exemption contained in section 32 of the DPA. One could

---

[29] Google under investigation by Met police, BBC News online, http://www.bbc.co.uk/news/10391096

[30] Dan Worth. Met Police clears Google over Wi-Fi data collection, http://www.v3.co.uk/v3-uk/news/1965782/met-police-clears-google-wi-fi-collection

[31] Joe Mullin. Google won't be prosecuted over Street View in Germany, http://arstechnica.com/tech-policy/2012/11/google-wont-be-prosecuted-over-street-view-in-germany/

[32] Durant v Financial Services Authority [2003] EWCA Civ 1746

probably argue that there is no need for them to publish the unpixillated faces of innocent bystanders in order to achieve their artistic purpose, but that would ultimately be something for the Information Commissioner to take a view on.

2.2. Creativity is knowing how to hide your sources

What remains is a discussion of the copyright implications of the works. Three issues need to be distinguished:

- did Valentine or Britnik violate copyright of the CCTV owner?
- Have they created copyright protected work
- Can they enforce this right?

CCTV footage in WI-Fi networks is protected under the Copyright Designs and Patens Act 1988 (CDPA) first and foremost a film, since a film is any recording in *any* medium from which a moving image may be produced. Since some CCTV cameras are increasingly "intelligent" in the sense that they react to environmental input and "decide" what and how (low quality/high quality; zoom v bird's eye view) they record, this means that the question of computer generated art *de lege lata* does arise. Although there is a special provision in the Act for computer generated literary, artistic, dramatic and musical work, film is not covered. While CCTV recordings are a very good example why the rationale behind this exclusion could be queried, a detailed analysis would go beyond the scope of this paper. For films, copyright is initially vested in the principal director and the producer. For CCTV footage, it is unproblematic who the producer is – the person who owns the cameras. Problematic for lawyers from continental Europe at least is however the issue of who the "director" of a film is, when the film is recorded automatically, without any artistic plan, and as noted above the "decision making" increasingly left to the machine or possibly the computer programmer who developed its software. UK law however does not require a film to be original to attract copyright (only that it is 'not copied' from a previous film), and generally does not follow the continental focus of the mental state of the artists in allocating rights. Rather, the fact that it is undoubtedly a film ensures in law that there is also a director (rather than the other way round), and in the case of CCTV footage, the only person that fits that role is again the owner who at least makes the decision where the camera will be placed. For him too, the fact that no "intentional" state is needed, that art emerges without an artist bearing her soul is no objection under the UK approach. If as in Valentine's case, a substantial amount of creative input comes from him and his actors, it may be (but not tested in court) that he would be designated as principal director, while the council is undoubtedly the producer (providing the cameras), and also a director but perhaps no only longer the principal director. In such case, The result is jointly owned copyright between Valentine and the CCTV owner under the statute, even though there is no joint plan or artistic vision between them. Valentine likely violated in this case the copyright interests of the producer when putting the video on his website without the producer's consent.

The situation is slightly more complicated in Bitnik's case. Here we are closer to a digital version of "appropriation art" or "objects trouve" – digital objects that they "find" through their CCTV sniffing "becomes" art by incorporating it into a performance. The unaltered footage from the CCTV cameras creates a film in which copyright is solely vested in the CCTV owner as producer and director. The "collage" of his footage with the images of the chessboard creates a new work of which Bitnik are again producer and director, but which violates the copyright in the original footage. Problematic is however the short part that

shows a member of the collective on the CCTV operator's film – taking out their computer in full view of the camera and enacting the game of "taking control". This could be first a dramatic work, which if considered original, may attract its own protection. Second, the film version of it has just as in Valentine's case a spy between producer role (still the CCTV owner) and director (the person deciding how the artists acts). That appropriation art poses copyright challenges is a well known fact.[33] Despite this, and some high profile public disputes about appropriation art and copyright (for example, in 2000, Damien Hirst reached an out of court settlement in relation to his 20 foot bronze sculpture 'Hymn', due to its similarity to the Young Scientist Anatomy Set) there are no court decisions that clarify the law. In the case of Surveillance Chess, an additional complication would arise from the difficulty to determine "what proportion" of the original was appropriated – after all, the camera records 24 hours every day, which raises the issue where "its" work starts and ends. Bitnik could also be tempted to argue that their work criticized the practice of CCTV surveillance, and hence benefit from the exception in section 30 CDPA that permits "criticism and review", a defence not available for the explicitly apolitical Valentine. However, at least in this case, the argument fails, since the provision requires that the work criticized has been lawfully made available to the public. With the CCTV footage of the London Underground, this is obviously not the case. However, had they hijacked CCTV footage in Edinburgh buses, which is transmitted directly to display screens in the bus for viewing by all, the situation might differ.

While therefore both Valentine and Bitnik violate copyright by using and publishing CCTV footage recorded on other people's machines, the resulting clips may also attract its own copyright. That they were born out of a rights violation, or possibly even criminal acts if we consider the above discussion of the Computer Misuse Act, is not an objection. However, this may cause difficulties in actually enforcing their right against infringers at least in England, under the doctrine *Ex turpi causa non oritur actio* - "from a dishonorable cause an action does not arise". It states that a claimant can't pursue a cause of action if it arises in connection with his own illegal act(s). A similar line of argument could focus on the "equitable" status of injunctions against copyright infringement. Here too a court may feel reluctant to order an injunction against a party violating Bitnik's or Valentine's copyright if it felt that given the production history of their clips, such a discretionary use of the state's power would be unmerited.

3. References

Schafer, B. 'Schlafwandelnd in den Überwachungsstaat?' Datenschutz und Datensicherheit. 8 483-489 (2009)

Ryan, P. S., War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics. Virginia Journal of Law & Technology,. 9, No. 7, (2004)

Berghel, H, Wireless Infidelity I: War Driving. Commun. ACM, 47, p 21-26 (2004)

Lawrence, E.; Lawrence, J , "Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking," Information Technology: Coding and Computing, 2004., vol.2, no., pp. 268- 273 (2004)

Kern, B., Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101 (2004)

Tsow, A, M. Jakobsson, L. Yang, S. Wetzel. "Warkitting: the Drive-by Subversion of Wireless Home routers ." Journal of Digital Forensics Practice, Vol. 1, No. 3, , pp. 179-192 (2006)

Bierlein, M "Policing the Wireless World: Access Liability in the Open Wi-Fi Era". Ohio State Law Journal 67 (5). (2006).

[33] Greenberg, Lynne, The Art of Appropriation: Puppies, Piracy, and Post-Modernism, 11 Cardozo Arts & Ent. L.J. 1 (1992)

Síthigh, D M "Law in the Last Mile: Sharing Internet Access Through Wi-Fi", 6:2 SCRIPTed 355, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.asp (2009)
Greenberg, L, The Art of Appropriation: Puppies, Piracy, and Post-Modernism, 11 Cardozo Arts & Ent. L.J. 1 (1992)

RCUK Centre for Copyright and
New Business Models in the
Creative Economy

College of Social Sciences / School of Law
University of Glasgow
10 The Square
Glasgow G12 8QQ
Web: www.create.ac.uk