Trustworthy Citizen-generated Images and Video on Social Media Platforms

Jessica Bushey, MAS
The Law of Evidence in the Digital Environment Project
University of British Columbia, Canada
jbushey@mail.ubc.ca

Abstract

The convergence of digital cameras into mobile phones with Internet connectivity and the proliferation of social media platforms for accessing, sharing, managing and storing digital images and videos has transformed news reportage and provided the opportunity for citizen journalists to capture and disseminate visual documentation, which shapes contemporary events, informs future decisions and over time, becomes part of the historical record and societal memory. Or does it? What are the obstacles to ongoing access and long-term preservation of citizen-generated content in social media platforms? This paper provides a multidisciplinary approach to exploring the trustworthiness of online content, utilizing literature from the fields of journalism and the law, as well as findings from archival studies on record-making and recordkeeping in the digital environment. Recommendations to citizen journalists are provided to assist in the capture and storage of trustworthy digital images in social media platforms.

1. Introduction

The incorporation of digital cameras into the professional practice of photojournalists in the 1990s enabled in-camera editing and increased the speed of transmitting digital images to news services via satellite phones. The adoption of digital technology by photojournalists also had an impact on the public’s belief in the trustworthiness of news photographs. Unlike fine art photography or photographic images used in advertising, which are guided by aesthetics and sales, news photography is presented as visual evidence of something or someone in the real world, and the truth of a news image rests in its correspondence to reality [1]. Instances of manipulation of news images by photojournalists prompted professional press associations to update their codes of ethics and publicly reprimand offenders [2]. Although academics and practitioners in the field of journalism concur that the photograph’s fidelity to the real world has been subject to speculation long before the transition to digital media, the impact of the shift from film-based to pixel-based visual reportage created fissures in the credibility of the institution of journalism.

In recent years, the availability of affordable mobile phones with high-resolution digital cameras and video capabilities coupled with Internet connectivity and the spread of broadband services throughout the globe has enabled a new form of visual reportage, citizen journalism, which is characterized by the non-professional status of the creators and the participatory nature of their involvement with the public event. Initial responses to the role of citizen journalists by professional photojournalists have been critical, emphasizing the lack of adherence to professional codes of conduct and an ignorance of professional photographic practices that incorporate metadata capture to establish the reliability and ensure the authenticity of the digital image or video [3]. Ironically, informal studies reveal that the blurry, amateur quality of camera phone images may increase the public’s confidence that the footage is authentic [3].

The current widespread use of photo and video-sharing sites (e.g., Flickr, Vimeo and YouTube) and social networking sites (e.g., Twitter and Facebook) to access, share and store digital images and videos created by individuals, regardless of their professional or amateur status, is gaining the attention of archivists interested in exploring the long-term preservation of user-generated content in social media platforms [4] [5]. This paper draws upon literature from the fields of journalism and the law that address the trustworthiness of digital images, as well as the findings of research conducted by archivists and information professionals on contemporary record-making and recordkeeping practices of individuals in the digital environment.

The multidisciplinary approach provides an opportunity to explore the phenomenon of citizen-generated content from different perspectives filtered...
through the lens of archival science and digital
diplomatics (i.e., the study of the nature, genesis,
characteristics, transmission, and legal consequences
of digital records) [6]. As a result of the abundance
of digital records, digital diplomatics arose out of
general diplomatics, which is a seventeenth century
discipline for examining a document and assessing its
trustworthiness [6]. North American archivists have
been introduced to general diplomatics through the
writings of Luciana Duranti, “Diplomatics: New Uses
for An Old Science,” and to digital diplomatics through
the findings of the International Research on
Permanent Authentic Records in Electronic Systems
(InterPARES) Project, a multidisciplinary research
collaboration aimed at developing the theory and
methods necessary for the preservation of authentic
electronic records [6] [7] [8] [9].

Archivists formed in archival science and digital
diplomatics are committed to the protection of records
as reliable and authentic evidence of past actions, and
have established through observational principles that
trustworthiness comprises reliability, accuracy and
authenticity; thus, a trustworthy digital image must be
simultaneously reliable, accurate and authentic [10]
[9]. If we want assurance of the trustworthiness of a
photograph we need to verify that the photograph is
capable of standing for the facts to which it attests (i.e.,
reliable), its content is precise, correct, and free of
error or distortion (i.e., accurate), and that the
photograph is what it purports to be and has not been
corrupted or tampered with (i.e., authentic) [6] [10]

This paper is part of a larger investigation being
conducted by the author towards her doctoral
dissertation on the trustworthiness of digital images
accessed and stored in social media platforms. Future
research activities include a web-based survey on
contemporary photographic practices in the online
environment and in-depth interviews.

2. Significance of Study

The study is significant for several reasons. First,
the study shows the extent to which the convergence
of cameras into mobile devices with Internet connectivity
has changed practices of news reportage, specifically
the creation, use and storage of digital images and
video, and the impact these changes have on record
trustworthiness. Second, the study reveals the evolving
legal implications of sharing, using and storing digital
content on social media platforms, specifically issues
of copyright and licensing of user-generated content
and ownership of member accounts. Third, the study
provides recommendations for citizen journalists
creating images and video documentation, as well as
archivists and information professionals considering
the acquisition and preservation of user-generated
content, which is accessed and stored on social media
platforms.

3. Literature Review

3.1. Journalism and Digital Images

Contemporary communication is increasingly
digital and visual [12]. Digital images and video are
made, accessed, managed and stored on a variety
of digital devices with imaging capabilities and in photo-
sharing and social networking platforms. The creation
and consumption of digital images is a global
phenomenon and scholarly research into how news
images are selected and circulated by image brokers
reveals the driving forces behind the digital
newsroom’s increasing demands for visual content to
fulfill an ever expanding myriad of online news
platforms [13]. Findings reveal that the economics of
the digital era are driving many of the decisions
regarding who creates news photographs. The results
of immediate transmission and global distribution are:
increased competition between professional
photojournalists and amateur “eye-witnesses” using
camera phones, shorter turn-around times and, in the
case of major news events, simultaneous reporting on
the event while it is occurring. These circumstances
present the opportunity for digital manipulation,
transmission errors, and incomplete captioning, which
lead to inaccurate and possibly falsified digital images
being published [14]. The inability to verify the
accuracy, reliability and authenticity of digital
photographs prior to publication does not stop the
images from being used in the mainstream media;
instead, they are disseminated with the caption:
“[Name of news producer here] cannot authenticate the
image.” [15]. Concern for the credibility of journalism
has arisen in response to digital technologies and the
unprecedented access to online publication and re-use
that social media platforms facilitate.

A major theme in the journalism literature is
methods for establishing reliable and authentic digital
images. One approach is the revision and enforcement
of professional codes of ethics for photojournalists,
specifically aimed at limiting the alteration and
manipulation of digital images [14] [16] [17].
Promoted by professional associations for visual
journalists, code of ethics emphasize the importance of
maintaining the integrity of an image’s context and
content in order to protect the trustworthiness of the
images and perpetuate journalists’ role as trustees of
the public [16]. Unfortunately, codes of ethics are limited in scope when applied to citizen journalists and individuals simply sharing their footage of a newsworthy event on social media platforms (i.e., accidental journalists) [17] [18].

The use of image metadata to provide technical and descriptive information, which contributes to the identity and integrity of the digital image and provides a method for ensuring the reliability of an image and establishing its authenticity has gained considerable traction with professional visual journalists and the visual imaging industry. All digital imaging devices and imaging software support the standard for technical metadata, Exchangable Image File Format (Exif) and many have adopted methods for photographers to add descriptive metadata, International Press Telecommunications Council (IPTC) Core & Extension to images through commercially available applications (e.g., all Adobe products) [19] [20]. The Exif schema captures technical information, including camera make/model, date & time, GPS data, image dimensions, and color space. The IPTC Core & Extensions schema captures descriptive information, including photographer name, subject and copyright/licensing terms. In 2007, the American Society of Media Photographers (ASMP) was awarded a Library of Congress National Digital Information Infrastructure and Preservation Program (NDIIPP) grant to publish dpBestflow, a best practices workflow for photographers working with digital images and video. The publication highlights both the IPTC photo metadata standard for describing images and image ownership, along with Exif as essential to establishing provenance and enabling discovery and use [21].

The International Press Telecommunications Council (IPTC) Photo Metadata Working Group conducted a survey on the removal of embedded image metadata from digital images by social media platforms from 2009-2013 as part of the larger Embedded Metadata Manifesto project [22]. The IPTC study analyzes the association of Exif and IPTC metadata with a digital photograph in the context of social media platforms, typically photo-sharing services (e.g., Flickr, Tumblr and Dropbox) and social networking services (e.g., Facebook, Google+ and Twitter) [28]. The study employed four scenarios to test whether or not image metadata remains linked to the photograph, including viewing the digital photograph online in the social media platform and downloading the digital photograph from the social media platform onto a personal desktop.

The findings of the IPTC Photo Metadata Working Group study reveal image metadata is inconsistently supported across social media sites and that the two most popular sites for sharing digital images, Flickr and Facebook remove embedded metadata from the image file header during procedures for uploading a digital image to the social media platform and downloading a digital image onto the desktop from the social media platform [22]. In the context of best practices that recommend the adoption of IPTC image metadata as a tool for effectively managing digital image collections and controlling their future use the research findings are unexpected and distressing [21]. Prior to the release of the IPTC Photo Metadata Working Group survey findings a number of social media providers were contacted and invited to respond, yet none did. Even after considerable news media coverage of the survey results, the major social media providers remain silent. The removal of image metadata during actions of uploading and downloading digital files into and out of social media platforms presents a real threat to establishing the trustworthiness of digital images in thousands of online collections.

The approaches discussed thus far have represented the perspective of professional visual journalists and organizations that operate within established news media frameworks. The concerns of professionals may be in opposition to those of accidental and citizen journalists, especially in regards to the role of image metadata and its removal by social media platforms.

The concept of privacy within the online environment is a complex and increasingly important issue. Many users of photo-sharing and social networking sites are becoming aware of the challenges to protecting individual privacy while engaging in activities of sharing online. The removal of Exif metadata from digital photographs, such as geospatial coordinates (e.g., GPS field) allows the individual to protect the location of where the photograph was taken. Individuals can remove the Exif metadata that is automatically captured by their digital devices by using an image editing application. It is not difficult to imagine a number of news worthy circumstances in which revealing the location of a person in the photograph, or the location where the photographer is based could jeopardize the life and liberty of participants.

A number of initiatives that embrace citizen-generated content have arisen, such as Allvoices (http://www.allvoices.com), Citizenside France (http://www.citizenside.com) and the Independent Media Center (www.indymedia.org). Allvoices invites individuals to submit original stories, images and videos to the site and then combines the submissions with related articles that are aggregated from mainstream news organizations. Contributors must abide by a lengthy Terms of Use policy, which outlines the rules and responsibilities governing the creation of
content that is free from copyright infringement and privacy restrictions [24]. Additionally, all content posted on the Allvoices site is curated by professional editors. The methods employed by Allvoices, those of a curatorial process in combination with related aggregated news sources, and the Terms of Use policy, should ensure credibility.

Citizenside France provides a news platform for citizen journalists, and professional photographers and videographers to submit original content. Citizenside utilizes a number of methods for sourcing user-generated content, including a proprietary interface, the Newzulu / Citizenside Social Media Reporter. A visit to the Citizenside homepage presents a number of news reports with the tag “vetted story” over each image. In addition to the Terms and conditions policy. Citizenside employs a number of methods for validating submissions, including editorial review and validation of content through social gaming capabilities built into the platform to ensure integrity and credibility prior to distribution [25].

The Independent Media Center is a network of independent media organizations and journalists dedicated to providing independent reporting on social and political issues [26]. Indymedia arose in response to the protests against the World Trade Organization conference in Seattle (1999). One of the underlying concepts of Indymedia is open publishing, which requires that the process of creating news is transparent to the readers [27]. In the context of trustworthy news images, the open publishing model provides the opportunity for readers to participate in the creation of the news, as well as its consumption. The audience is free to investigate the accuracy of a news story uploaded to an Indymedia site and provide additional evidence that contradicts or supports the earlier account. In many respects, these types of activities reflect traditional approaches to ensuring credibility in news reportage, such as fact-checking, eye-witness corroboration, cross-referencing with other data, and contacting the source. The online environment presents readers with access to digital applications to assist in analyzing news images to determine prior use (e.g., TinEye, reverse image search tool) and digital manipulation (e.g., FotoForensics, an error level analysis tool).

A more recent development is that contributors to Newzulu / Citizenside can insert #newzulu in their Twitter and Instagram content and the news media platform will acquire and validate the submission. The massive popularity of social media platforms establishes photo-sharing and networking sites as the defacto providers for images and videos that “go viral.” As a result, citizen journalists and professionals use Twitter to disseminate newsworthy images in real time on a global scale – evident in the Arab Spring (2011) and recent political protests in Turkey, Ukraine and Thailand. News organizations that integrate technological platforms to enable the sharing and validation of user-generated content, such as those being employed by Citizenside are providing innovative solutions to curating the deluge of digital content. It is important to remember that all the initiatives discussed in this section require the individual to be informed of their existence and the different protocols for submitting content prior to capturing news worthy images.

3.2. Law and Digital Images

Since its inception in 1826, the photograph has played an important, albeit controversial role as documentary evidence of past events, persons and places [28]. Photography’s early association with science and accurate reproduction attributed to the medium by its mechanical production and seeming lack of human intervention positioned it as a powerful tool for documentation. The photograph’s capacity to extend the power of human observation made it useful in the areas of law enforcement. The application of photography in the law was predicated on the belief in the accuracy, reliability and authenticity of photographs as visual recordings of the real world [29]. This belief was based, to an extent, on the Anglo-American justice system’s approach to admitting photographs as documentary evidence. Since the early 1900s, statutory and common law evidence rules have allowed photographs to be introduced as evidence of facts related to legal proceedings, albeit with increasing controls over their admissibility.

A major theme in the North American legal literature is the inadequacy of existing rules for identifying and authenticating evidence when dealing with digital photographs and more recently, images accessed and stored in social networking sites [30] [31] [32]. Concerns are being raised by litigators and legal scholars regarding the ease of digital manipulation and the potential for falsified photographs to be admitted into evidence at trial [33] [34]. It is recognized that the laws being applied in the digital era are based on a paper environment. In response to the ubiquity of digital documents, images and videos in contemporary business and personal activities, the legal community is discussing approaches to managing digital evidence and to establishing its authenticity. The following section highlights key publications, memorandum opinions and cases that address digital evidence, as well as a research project on the nature of digital evidence.
In 2007, the United States Federal Judicial Center authored, “Managing Discovery of Electronic Information: A Pocket Guide for Judges,” which discusses how electronically stored information (ESI) includes digital images and information generated by software and systems that exchange digital information (e.g., metadata), and encourages judges to actively manage cases involving ESI instead of waiting for the parties to argue the matter [35]. The first edition of this publication followed the 2006 amendments to the Federal Rules of Civil Procedure. Considered an ESI primer, the second edition was released in 2012 and reorganized into a question and answer format [36].

The opinion provided by Magistrate Judge Paul Grimm in Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007) is referred to extensively in the legal literature regarding the issue of social media and digital evidence [34]. Judge Grimm suggests two approaches to authenticating ESI: the first requires a witness testimony to explain the process of how ESI is created, acquired, maintained, and preserved (without alteration), and the second requires a witness testimony to identify the process by which ESI is produced if a system is relied upon to do so. Judge Grimm also suggests that metadata should be treated as a distinctive characteristic that shows the date, time, and identity of the creator of a digital record [34].

In light of Grimm's judicial opinion it is difficult to determine how a member of a photo-sharing or social networking site would establish the process by which ESI is produced and, in circumstances where the image metadata is stripped-out of digital photographs, it would be impossible to use it to support or refute a legal claim. It is more likely that the approaches suggested by Judge Grimm would require the testimony of the service provider and assurance that the social media platform does not alter the metadata embedded in the original file of the digital image. The legal literature that addresses evidence in networked environments specifies that one of the challenges to authenticity is identifying who or what generated the digital document and determining whether safeguards have been implemented to assure continuing accuracy and integrity of the document [37].

In 2011, Magistrate Judge Kristen Mix published an article entitled, “Discovery of Social Media”, in which she states that the recent political events in Egypt demonstrate the importance of social media for the legal profession and society at large [38]. In her article, Judge Mix explores the legal obstacles to accessing content in social media platforms and using that content at trial. She highlights the Canadian appellate court approach to content on social networking sites, which dismisses expectations of privacy in the shared environment and obliges a party to identify and produce postings that relate to the matter at hand [39]. This approach places the onus on the user to produce content and avoids the formal request to the provider for the content through a subpoena. As Judge Mix notes, most social media providers include a section in their Terms of Use policy that outline their obligation to respond to subpoenas. Unfortunately, courts in the United States are inconsistent in their rulings on access to social media content, at times protecting some types of social media content from subpoena under the Stored Communications Act (SCA). As a result, it is difficult to determine what types of social media content (e.g., wall posts vs. messaging services) may be accessed and admitted as evidence at trial. Additionally, users of social media platforms are generally unaware of the information contained in Terms of Use agreements with social media providers, which impacts how they use the service and their expectations of privacy.

A major theme in the legal literature is the issue of legal agreements between social media platforms and their members, specifically the Terms of Service [40]. The legal community refers to the type of contracts used by social media providers as “clickwrap” and “click-to-agree,” because the potential member must consent to the terms and agreement by starting to use the software or, by clicking a box onscreen that reads, “I agree.” The terms and conditions may be presented as a single document, or they may be comprised of a number of different documents, including Privacy Policy, Acceptable Use Policy, Terms of Use (ToU) and Service Level Agreements (SLA). Legal scholars suggest that for different reasons, the majority of people enter click-to-agree contracts without reading the fine print terms; even though, upon inspection, it is evident that a number of clauses are included that significantly limit member’s legal rights [40]. Furthermore, social media service providers retain the right to change their terms at any time and at the company’s discretion.

The issues raised by the literature on Terms of Service agreements between social media providers and their customers include intellectual property licensing, control of user-generated content and future access to social media accounts. Both Facebook and Instagram (purchased by Facebook in April 2012) include language in their agreements that allows for the licensing of any content posted through the service that is not explicitly marked as private; however, the ability to determine what constitutes private or public content in social media services can be challenging. The social nature of photo-sharing sites encourages members to share their content with as many friends as possible, providing the opportunity for comments, tags and
ratings, which are all activities that may transform a digital photograph into public content. The literature emphasizes that the boundary between social networking and hosted site services is difficult to determine [41] [42]. In the context of citizen-generated content that may be used by news services it is very important that the boundaries of legal ownership and use are clearly stated in the Terms of Service and that both the service provider and the social media member understand the implications for present and future use.

In late 2012, the photo-sharing service Instagram received media attention for changing its Terms of Use (ToU) without alerting its members. The change gave Instagram the perpetual use of photographs and videos stored on its site, as well as unlimited rights to license the images to any and all third parties. The license persists even if the member downloads their content off the site and terminates their account [43]. In January 2013, the foreign news association, Agence France Presse (AFP) was held liable for copyright infringement when it used photographs of the Haitian earthquake that photojournalist Daniel Morel had originally taken and posted on his Twitter page [44]. AFP asserted that Twitter’s terms of service granted an implied license for AFP to use Morel’s photographs, and that AFP was a third party beneficiary of the contract between Twitter and Morel [45]. The trial court rejected AFP’s argument and District Judge Nathan stated that Twitter is the only party granted license to use their member’s content. Morel was awarded 1.2 million dollars in damages [46].

These examples reveal the need for organizations and individuals that use social media platforms to access, share and store digital images and videos to review the ToU in order to determine if the licensing clause simply asks for the rights necessary to operate the service (e.g., Vimeo needs the right to create derivative works from your video in order to encode it into different formats) or, if it asks for the rights to sublicense user-generated content for monetary gain. Issues regarding the licensing and future use of user-generated content are important because they may impact the ability for archives to access and preserve social media content [4].

Lastly, the Law of Evidence in the Digital Environment (LEDE) is a 3-year collaborative research project between the Faculty of Law and the School of Library, Archival and Information Studies (SLAIS) at the University of British Columbia, Canada, which focuses on the ability of rules governing the admissibility of evidence to deal with the challenges presented by digital information [47]. In addition to case law review, LEDE researchers have conducted a survey of lawyers and professionals working with digital evidence, which produced findings revealing that email, social media, text messages and digital photographs were the types of digital evidence in which respondents encountered the most issues. Additionally, survey respondents selected personal information and protection of privacy and e-discovery as the two areas in which current laws and legal proceedings are insufficient to adequately answer legal challenges involving digital evidence. Follow-up interviews are currently being conducted to explore identified issues in more depth. One of the objectives of the research project is to propose new and revised rules for the law of evidence with enough flexibility to accommodate future changes in digital technology.

4. Studies in Archival Science

Archivists are at the forefront of investigating the trustworthiness of digital records and the issues concerning digital records and data entrusted to the Internet. In the early 1990s the adoption of digital technologies for procedures of creation, use, maintenance and storage of recorded information prompted archivists to undertake interdisciplinary research to investigate the record-making and recordkeeping practices of creators of digital materials for the purpose of informing acquisition, management and preservation activities performed by archivists and cultural heritage professionals. Unlike traditional systems, in which procedural controls are established over the creation, management and preservation of records to ensure their reliability, accuracy and authenticity; the digital, networked environment is more volatile and digital records are more vulnerable to unintentional loss, alteration and corruption during routine activities performed by the creator and the preserver [48].

The following section focuses on archival studies that explore the creation, management, use, storage, access and preservation of digital materials with cultural, administrative, scholarly and personal value. The selected studies are grounded in the fundamental archival principles of provenance (i.e., records from a common origin should be managed together as an aggregate unit and should not be intermingled with records from another creator) and original order (i.e., archival arrangement of records should reflect the original organization used by the creator), as well as chain of custody (i.e., a documented succession of persons or offices responsible for the care and management of the records from the moment of creation onward). The cumulative findings of these studies are forging a new direction for contemporary archival theory and practice, one that incorporates methods and tools developed by auxiliary disciplines, such as digital diplomacy and digital forensics (i.e.,
the use of scientifically derived and proven methods toward the identification, collection, validation, analysis and preservation of digital evidence) [6].

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) Project 1, 2, and 3 (1999 – 2012) developed an intellectual framework and methodology based on archival science and digital diplomatics for understanding the long-term preservation of authentic records, created and/or maintained in digital form; and provided the basis for standards, policies and strategies for ensuring the longevity of digital records across systems and over time [49] [50]. In 2006, as part of InterPARES 2 a survey was conducted, in which the practical aspects of how professional photographers create and manage their digital photographs as reliable records, and preserve their authenticity over the long term were explored [51]. The findings of the survey revealed the importance of the type of storage media and the persistence of image metadata for ensuring the authenticity of digital photographs [52]. Image preservation activities included (in order of frequency): selecting storage media (e.g., CD-R, DVD-R and external drives); designating file formats for originals and surrogates (e.g., RAW, TIFF and JPEG); unique file naming; and using software with batch metadata capabilities [52]. Additional comments provided by survey respondents emphasized their reluctance to publish digital images online without additional safeguards, such as watermarks, copyright statements and descriptive metadata (IPTC) to establish legal control over the re-use of their content [52].

Since the survey was conducted, a great deal has changed in social attitudes towards ownership and use of digital images accessed and stored in the online environment, as well as the technology available to professional and amateur photographers. Contemporary photographic practice, as seen in the activities of citizen journalists, relies on cameraphone capture and direct upload to social media platforms. The immediacy and mobility that characterize accidental and citizen journalist activities leave little room for back-up procedures on external media or extensive application of metadata to images prior to dissemination. The InterPARES 2 study highlights how photographic practice is shaped by individual habits, social interaction, the technological environment, and legal requirements. A point that is all too evident in the global adoption of mobile phones as cameras – a simple example of convergence and convenience.

The Digital Lives Project (2007-2010), explores the theoretical and practical aspects of curating personal digital objects (i.e., manuscripts, images, videos etc.) over the entire archival life cycle (i.e., creation through preservation) and their findings reveal that widespread adoption of social media platforms for sharing and storing personal digital collections indicates an area for potential future collaboration between archival institutions (mandated to preserve public and private records) and social media service providers in an effort to offer services that support the long-term preservation of authentic online content [53]. Led by the British Library, in partnership with University College London and the University of Bristol, the Digital Lives Project produced a discussion paper on the legal and ethical issues introduced by user-generated content and approaches to acquiring and preserving personal digital archives [54]. In regards to the role of archival repositories acquiring, providing access and preserving personal digital archives, the key legal issues identified by the study are copyright and privacy laws. These two areas are impacted by new technologies, public expectations of access, and laws suited to the paper environment.

Both copyright and privacy laws are based on a specific jurisdiction, which can become complicated when applied to social media platforms. For example, in *Douez v. Facebook*, the British Columbia’s Supreme Court released a decision granting the Plaintiff’s motion to certify a claim for statutory breach of British Columbia’s Privacy Act against the defendant, Facebook [55]. The case deals with privacy and jurisdiction. Facebook argued that their Terms of Use agreement states that California is the legal forum selection for disputes; but the images used by Facebook without consent belonged to members who live in British Columbia, making the breach of privacy an issue for the BC Supreme Court. In the concluding statement, the Court emphasizes the importance of policing privacy violations by multi-national social media service providers [56]. At this early stage it is difficult to determine what the impact of the online environment will be on copyright laws regarding orphan works (i.e., works in which copyright holders cannot be located) and fair use for libraries and archives. However, it is clear that digital images uploaded to social networking platforms can be shared with millions of people in a matter of minutes and that many providers and users adopt the attitude that social media content is in the public domain and its reuse is fair use [57].

Two recent publications aimed at assisting archival repositories in the acquisition and management of digital collections; provide archivists with useful workflows and the integration of digital forensic tools and practices to access data on storage devices. The 2013 Council on Library and Information Resources (CLIR) report, “Born Digital: Guidance for Donors, Dealers, and Archival Repositories,” addresses the key issues and stages in acquiring and transferring born-
digital materials to archival repositories [58]. This is a timely and valuable publication; however, it does not address user-generated content stored in photo-sharing and social media platforms. Some of the concerns that are raised in the report, such as protecting the integrity of digital files by not copying or removing them from their original sources, or the need to clear third-party licensing terms, should be re-examined in light of digital collections accessed and stored on social media platforms in which image metadata may be stripped-out of files during transfer into and out of social media services and licensing agreements may not be fully understood by individuals due to complex terms and conditions [58]. The 2013 BitCurator report, “From Bitstreams to Legacy: Putting Digital Forensics into Practice in Collecting Institutions,” is the result of the first phase of the research project BitCurator (2011-2013), which is an effort to build, test, and analyze systems and software for incorporating digital forensics methods into the workflows of collecting institutions (i.e., archival repositories, libraries and museums) [59]. The report discusses the growing importance of forensic tools and techniques to care for digital collections in libraries and archives, providing a comprehensive overview of the literature to date, supporting research projects, case studies and best practices. Both the CLIR and Bitcurator reports address the challenges to accessing and preserving digital records that are stored in a computer or on external media (e.g., discs, external drive). This reflects documentary practices to date, for example, most organizations and individuals do not expect archival institutions to access their social media account and download the contents… yet.

An approach to accessing and preserving user-generated content stored in social media platforms is discussed in “Archiving large amounts of Individually-created Digital Content: Lessons from archiving the Occupy Movement”, a project conducted by students of New York University’s Moving Image Archive and Preservation Program (MIAP) in 2011 [4]. The project explores collecting and preserving the media generated by citizens involved with the Occupy movement. As the project moved forward, a number of issues were identified in the activities of citizen journalists and activists, which placed the digital images and videos being created at-risk for archival preservation. For example, activities of capture and upload to social media platforms did not include the addition of metadata to identify the photographer, subjects, action, or date; copies were not made for back-up; and in some instances the original images stored on the cameraphone were erased in response to personal security concerns. To address these issues, MIAP students created documentation to inform and guide photographers, such as the “7 Tips to Ensure your Video is Usable in the Long Term,” which recommends keeping original footage, making the recording accessible, providing context to make it verifiable, and taking steps towards preserving it [4]. The findings of the study reveal the loss of image metadata during upload from mobile devices (iPhone, Android and Canon t2i) to social media platforms (YouTube, the Internet Archive and Vimeo), confirming the findings from the IPTC study, which was limited to still photography [4].

MIAP Professor, Howard Besser stresses the importance of citizen-generated content as culturally significant as a whole, but challenging for archival institutions to collect due to the massive volume, variety of file formats, lack of identity and integrity metadata, and dispersion of media across different platforms. It is clear that sharing the expertise of archivists with creators is an important step in solving the problem of how to organize, preserve, and provide access to large amounts of user-generated content in the future. However, an additional issue raised by the project that is unique to content generated by activists and by default, to the images and texts generated by citizen and accidental journalists reporting from areas of conflict and war, is the potential unwillingness of creators to cooperate with “institutions” interested in preserving social media content. The participants of the Occupy movement were wary of trusting the New York University’s Tamiment Library because it represents a traditional institution and there were fears that the materials gathered by archivists could be used in legal actions against the protesters [60].

It is important to recognize that the needs of citizen journalists and activists may conflict with the requirements set forth by archivists to ensure that archival records can be linked by their provenance, are presented according to their original order and can be proven to have an unblemished chain of custody. The digital environment disrupts traditional notions of ownership, privacy, and permanence; yet, the necessity of providing future users of digital archives with an assurance that the records they are consulting are trustworthy necessitates an effort to resolve these issues.

5. Recommendations

This paper examines the issues that impact the trustworthiness of citizen-generated content in social media platforms, with a focus on the factors that support or hinder the reliability, accuracy and authenticity of digital images and video. As record-making and recordkeeping activities continue to evolve, the value of visual reportage held in photo-
sharing and social networking sites as potential records to be acquired and preserved by archival institutions will require the effort of both creators and preservers. A product of both the InterPARES 2 project and the Archiving and Preserving the Occupy Wall Street movement project are guidelines to assist creators in making choices at the outset of their record-making activities that will ensure the usability and longevity of their digital records for the long term [61] [62]. The guidance provided by The Digital Lives Project, the CLIR report and the BitCurator Project supports collecting institutions actively acquiring, managing, preserving and providing access to digital materials.

The recommendations provided in this section are intended to assist citizen journalists who are creating visual reportage using mobile devices and sharing and storing their digital images and videos in social media platforms. The recommendations broadly address the issues identified in the literature and archival studies, as well as provide specific solutions that utilize currently available tools and outreach opportunities.

Recommendation 1: Citizen journalists should ensure that their mobile devices for image capture are Exif compliant and that the device is working properly. By selecting a standard metadata specification that is interchangeable, extensible and consistent, there is an increased assurance that the visual documentation will remain viable and interoperable for the long term. This is especially critical in regard to technical metadata and the proper presentation of the content of digital images on future systems. It should be noted that in rare circumstances, citizen journalists may choose to delete Exif metadata from online images that reveal personally sensitive information, which could place them, or their subjects in the image in danger.

Currently available tools for viewing and editing Exif metadata embedded in digital images are: Jeffrey’s Exif Viewer (http://regex.info/exif.cgi), View and Remove Exif Online (www.verexif.com) and Exif Remover (www.exifremover.com).

Recommendation 2: Citizen journalists should add IPTC Core & Extensions metadata to their images to describe the event being recorded. By selecting a standard metadata specification that is interchangeable, extensible and consistent, there is an increased assurance that the visual documentation will remain viable and interoperable for the long term. Additionally, citizen journalists who want to be financially compensated for their work, or recognized as the photographer need to ensure that their images and videos can be accredited to them after the digital material has been shared (e.g., retweeted). The currently available app Tagg.ly (www.tagg.ly), has been created to provide context to social media by stamping it with metadata. After setting-up the app, you simply take a photo or video with your mobile phone and Tagg.ly automatically adds the metadata to the photo and to the access data. The app works with iPhone and a future release is planned for Android phones.

Recommendation 3: Citizen journalists should review the terms and conditions agreements of social media service providers. Special attention should be paid to terms that are too far-reaching, specifically the granting of perpetual use licenses to the service provider without any right to termination and granting the service provider the right to license user-generated content to third parties for any and all uses. Currently available through the American Society of Media Photographers (ASMP) are a concise collection of guides available for download, “Utilizing Social Media for Your Business – Marketing & More”, “Know Your Rights on Social Media – Legal Considerations & More”, and “The Photographer’s Guide to Twitter” [63].

Recommendation 4: Citizen journalists should select image capture devices, imaging software and social media platforms that do not remove associated metadata from digital image and video files. Best practices for record creation recommend storing all original image and video files with their metadata in a secure location (e.g., offline external drive, redundant cloud storage service) and only uploading copies to social media platforms for dissemination. Ultimately the creation of a social media policy regarding the handling of image metadata, in which social media providers, photographers, and archivists could contribute as stakeholders would be ideal. Until then, individuals interested in pursuing citizen journalism should explore relationships with organizations such as Citizenside / Zulunews, in which the news platform has been engineered to harvest and validate user-generated content from social networking platforms – Twitter and Instagram.

Recommendation 5: Citizen journalists should contact an archival institution to discuss potential methods for selection, deposit and/or transfer of their digital visual collections as early as possible. The U.S. National Digital Stewardship Alliance (NDSA) has recently embarked on a project to discover at-risk digital content and engage stakeholders in the process of acquiring, preserving and providing access to that content. Led by the NDSA’s Content Working Group, a case study on citizen journalism is underway, in which the reportage of citizen journalists (e.g., blogging, tweets, Facebook posts) has been identified as having historical value [64]. One of the goals of the project is to raise awareness at local, state, national and international levels of the value of citizen journalism content, and communicate the need to preserve it.
6. Conclusion

This paper presents a multidisciplinary approach to exploring the trustworthiness of citizen-generated content in social media platforms. The proliferation of photo and video-sharing sites and social networking sites demonstrate the global practice of real-time, image-driven communications. Nowhere is this more evident than in contemporary news reportage, in which proximity and connectivity are the determining factors. As more activities are experienced online, the significance of social media platforms will continue to grow and the volumes of digital images and videos held within individual member accounts will increase exponentially. The recommendations provided in this paper are applicable to the broader population living “digital lives” and by default, relying on social media platforms to provide ongoing access to their digital images and collections. Unfortunately, the stripping-out of technical and descriptive image metadata by social media platforms present a serious risk to the trustworthiness of digital collections; and the far-reaching terms and conditions agreements of social media service providers present an obstacle for future access and preservation of digital collections by archival institutions. These issues need to be discussed further and an exploration into user’s expectations of ongoing access and long-term preservation of digital collections in social media platforms needs to be conducted.

7. References


