The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance

Mir Adnan Ali and Steve Mann
Department of Electrical and Computer Engineering
University of Toronto, 10 Kings College Rd, Toronto, ON, CANADA

***Abstract*—Surveillance is a French word that means "to watch from above" (e.g. guards watching prisoners, police watching citizens, etc.). Another form of veillance (watching) is sousveillance, which means "to watch from below". Whereas surveillance often means cameras on large entities (e.g. buildings and land), sousveillance often means cameras on small entities (e.g. individual people). The importance of sousveillance has come to the forefront recently with advancements in wearable computing and AR (augmented or augmediated reality).**

We characterize sousveillance from both an economic and moral perspective. We argue that societies that reject sousveillance will be impoverished, relative to those accepting sousveillance. We further argue that sousveillance as a form of social action has positive survival characteristics, so that in the long run, assuming that social and technological trends continue, the widespread adoption of sousveillance is inevitable.

I. Introduction

A. Surveillance

The primary definition of the word **"surveillance"** is:

- "**a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like**: *The suspects were under police surveillance.*" [1]

The etymology of this word is from the French word "surveiller" which means "to watch over". Specifically, the word "surveillance" is formed from two parts: (1) the French prefix "sur" which means "over" or "from above", and (2) the French verb "veiller" which means "to watch". The closest English word is "oversight", although the latter has two meanings: (1) watching from above, as in "oversight committee" and (2) an omission or error, as in "that was an oversight on our part". Because the French word gives less ambiguity and flexibility "veillance" will serve as the root of a set of categories.

B. Sousveillance: Putting cameras on people

A more recently coined word is the word "sousveillance", which is an etymologically correct opposite formed by replacing the prefix "sur", in "surveillance", with its opposite, "sous" [2], [3], [4], [5].

Sousveillance is typified by cameras borne by people, e.g. hand-held or wearable cameras controlled by the wearer, and not worn on behalf of another party [6], [7].

C. Specific definition of surveillance and sousveillance in the context of this work

In the present analysis, we select a particular meaning to focus on the social, and consequently informational, asymmetries of parties involved in veillance. As adjectives, these words are *indicative* of the properties of the object they describe. However, the use of the adjective does not imply that the object so described can only be used to accomplish the action indicated by the verbal form – in other words, a "surveillance camera" can be used for sousveillance, and vice versa. The meaning of interest here is the verbal form, where veillance is *conscious action*.

While commonly used to refer literally to visual signals, the meaning of *surveillance* and *sousveillance* have been generalized from vision to other sensory signals such as sounds, and observational data in general. For the purposes of this work, we specificize our definition to exclude non-artifact producing veillance; that is, direct observation without transmission (i.e. translation in time or space) is not considered veillance in this paper. Therefore, the definitions used here are:

> ***surveillance*** *v.* Monitoring undertaken by an entity in a position of authority, with respect to the intended subject of the veillance, that is transmitted, recorded, or creates an artifact.
>
> ***sousveillance*** *v.* Monitoring undertaken by an entity **not** in a position of authority, with respect to the intended subject of the veillance, that is transmitted, recorded, or creates an artifact.

In these definitions, an entity having a *position of authority* means that the possessor of that authority has both ability and legitimacy, in a normative sense [8], to enforce their will. The definitions used here are concerned with the *intentions* and *purposeful actions* of the parties involved in veillance, as distinguished from other sociological frameworks such as *actor-network theory* or ANT [9], where inanimate objects are considered actors in their own right. There is no logically consistent way to ascribe legitimacy, intentions, or desires to inanimate objects, nor are we concerned with situational outcomes from the perspective of machines.

D. Model of Analysis

The model of analysis we use comes from an engineering perspective, namely Humanistic Intelligence (HI), as shown in

978-1-4799-0929-2/13/$31.00

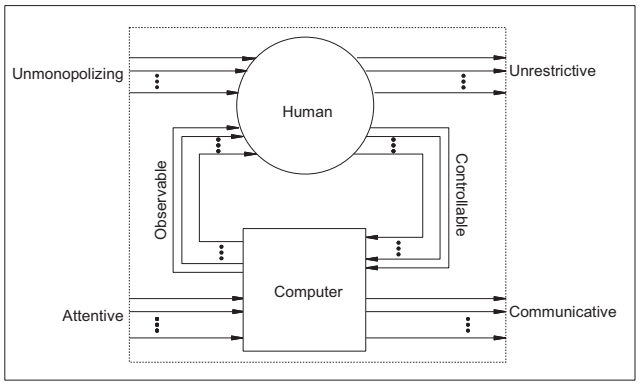

Fig. 1: A single participant in our system model, in terms of *Humanistic Intelligence* (HI). Each path defines an HI attribute, enumerating the six signal flow paths for intelligent systems embodying HI. This framework places the human in the executive position, in that the machine is always observable and controllable by the human component. The system is intrinsically configured to meet the needs of the human inside the cyborg.

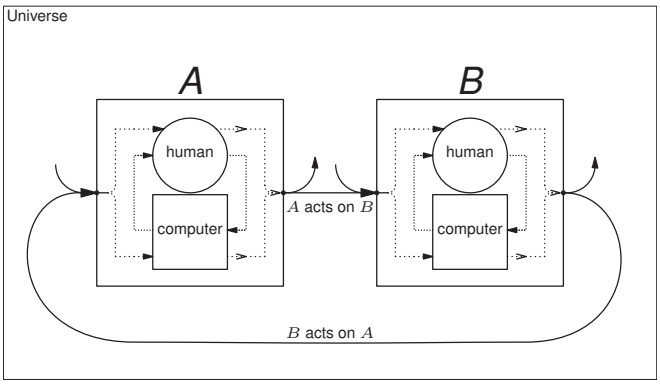

Fig. 2: Smallest universe supporting social action, with cyborgs A and B interacting with each other and their environment. From a signal-processing point-of-view, "to act on" refers to altering the input signals to a participant. However, from an economic perspective, this information flow is only the basis or substrate for transactions. Adding more participants maintains a fully-connected topology, and each participant may be aware of and may act on any other.

Fig. 1. The fundamental perspective of HI is that mechanistic systems are not of interest for any "inherent" capabilities, but rather they are of interest in the context of the *directed application* of any device towards ends determined by a human, who *uses* devices as a means toward a *conscious* end [10], [11, p. 68].

We use HI as our preferred embodiment of sousveillance, since the attributes of a system using HI are of economic consequence due to the costs involved – not merely the financial cost of the apparatus, but also in terms of the resources represented by the HI pathways. Specifically, the "cognitive bandwidth" (i.e. the attention needed to complete a transaction) of a participant is a significant resource in itself. This implies, for example, that a system that requires a user to complete 10 steps synchronously (e.g. unlock smartphone, swipe, swipe, launch application, select payee, input amount, initiate transaction, review transaction, confirm transaction, lock smartphone) is much less likely to succeed, due to its greater *transaction cost*,[1] than one embodying HI, which may only take a single asynchronous step to complete the same transaction (e.g. an unmonopolizing prompt, triggered by the situational awareness of the HI device, requesting a payment of $4 to The Coffee Shop and requiring only an asynchronous binary response to accept or decline the payment). The same logic as for a financial transaction also holds for sousveillance, in that sousveillance accomplished using an HI system may require no conscious effort at all, and so less use of scarce resources, thus improving efficiency, and therefore again reducing transaction costs.

In this model of system analysis, human and machine are considered as a single unit – the human's capabilities may be augmented or diminished by the devices they are joined with. "We prefer to regard the computer as a second brain, and its sensory modalities as additional senses, which through synthetic synesthesia are inextricably intertwined with the wearer's own biological sensory apparatus" [16].

In this way, human-centric values (such as preferences, motivations, objectives, sense of justice, interests) preserve their usual meanings, allowing us to reason about them. In particular, the focus on human participants and their objectives also affords us consistency in reasoning about the future – capabilities may shape specific desired outcomes, but the underlying motivations (and the mechanisms that generate them) remain the same, and are distinctly human. To make the lack of distinction between human and cyborg (human+machine) clear, we note that all humans are equal in *worth*, but no two humans are equal in *function*. That is to say, cyborgs merely add to the natural and already existing variability of human abilities; they do not form an independent category of life-form. Furthermore, since sousveillance and surveillance are *social* actions, as in Fig. 2, a universe consisting of a lone cyborg cannot give rise to surveillance nor sousveillance; this result differs fundamentally from the ANT model, where inanimate objects are also considered *actors* in their own right.

E. Propositions

To provide some clarity, we note the following propositions that follow directly from our definition of sousveillance and surveillance. All veillance is purposeful action. All sousveillance and surveillance is purposeful *social* action, where *society* is two people, or one person plus a society. Therefore, a camera inadvertently left on is engaged in neither sousveillance or surveillance,[2] and a universe consisting of only a single being supports neither sousveillance or surveillance.

Consider a person, engaged in sousveillance, producing artifact X. Later, X is turned over to the authorities in

[1]While here we mean "transaction cost" in a very literal sense, in general we mean the classic concept as introduced by Commons [12] and developed by Coase [13] and Williamson [14]. In particular, while we acknowledge the importance of trust in enabling efficient transactions, we share the perspective that mitigation of opportunism [15] provides many of the same advantages. See Sec. II-C. Furthermore, we see the cost of enforcing property rights, e.g. via courts or arbitration, as non-negligible. We examine this in more detail in Sec. II-E.

[2]Later viewing of the recording may be some form of sousveillance or surveillance, however at the time of capture there is no intention and therefore no sousveillance or surveillance.

support of a criminal investigation, to augment their existing crime-scene artifacts. The authorities are then engaged in surveillance based on X, even though X is a direct product of sousveillance.

Conversely, for example, consider the situation that government surveillance artifact Y is leaked, perhaps in support of publicizing government corruption, unjust use of violence, or incompetence. Then, artifact Y is being used for sousveillance – even though the original act producing Y was surveillance.

II. Economics of Sousveillance

Economics, as defined by the Merriam-Webster dictionary, is "a social science concerned chiefly with description and analysis of the production, distribution, and consumption of goods and services". Due to the corporeal reality of humans, economics can be considered in terms of of human action. We define *action* as purposeful and goal-driven behavior, and not reflexive or instinctual behavior, which is conceptually excluded from the category "action". Economics, therefore, is a study of human action [17, Ch. 1].

Due to the fundamentally social nature of humans, economics has always been concerned with the actions occurring between parties, which we distinguish here as *social action*, hence the categorization of economics as a *social* science.

While the general premise of the high economic value of relationships, and the consequent division of labor and specialization it affords, has been recognized in broad terms for millennia [18, p. 103], more recent work has illustrated the mechanisms humans use to gain both efficient production and use of resources.[3]

As we will discuss in greater detail below, in Sec. III, economics profoundly affects the ability of man to perform morally positive actions, because such actions typically require *resources*, and more generally, *prosperity*. "Prosperity" in economics typically refers solely to material wealth. However, in this work we use the term in the more general English-language sense that includes wealth, physical health, security of person, emotional well-being, personal growth, and so on. The etymology of prosperity is "good fortune", but this connotes a degree of fatalism – i.e. prosperity is something that occurs solely by external forces. We consider prosperity in the sense of "flourishing", that for any individual depends on both correct internally-directed action, and favorable external environmental conditions.

We take as well-established that general prosperity requires specialization of labor [20]. This implies further that group size is critical for material prosperity, since larger groups functioning well can specialize to a much greater degree. To profit from the properties of large group size, the participants must be able to engage in exchange. This necessitates that participants in a large society limit themselves in particular ways, so that emotions such as *trust* and *empathy* can be established, and that outcomes such as *justice* can be expected. Large-group cooperation, in the form of transactions, is a fundamental requirement for societal prosperity.

A. Sousveillance, trust, and transactions

A trustworthy party is one that will not unfairly exploit vulnerabilities of the other parties in the relationship. The reason trust is important economically is to enable transactions to proceed with a minimum of transaction costs. Trust is linked to identity, and the reputation ascribed to that identity. Examples of the benefits of trust-based transactions in cost and efficiency, dating back over a thousand years, can be found in the ancient Muslim "Hawala" transfer system[4] [21], [22], [23] and the Jewish Maghribi trader's coalition [24]. The fact that Hawala money transfers are still used today, and remain less expensive than modern electronic banking systems, provides attestation of the economic advantage of trust-based transactions. An excellent review of trust from an ethical perspective is in [8, p. 308], from which we quote:

> *"The necessary conditions for a trusting relationship... are:*
> *1) Interdependence: at least one party in a trust relationship must be dependent on at least one other party in order to accomplish a goal.*
> *2) Vulnerability: at least one party in the trust relationship is vulnerable to the opportunistic behavior of another party in the trust relationship.*
> *3) Risk: as a result of this vulnerability, the interests of at least one party in the relationship are at risk.*
> *We can then define a trust relationship as one of interdependence where at least one party is vulnerable to the opportunistic behavior of least one other party to the relationship but where nonetheless the vulnerable party voluntarily accepts the risks of its vulnerability."*

In the present analysis, we can assume that potentially transacting parties already have some degree of interdependence, hence the attempt to transact. With respect to sousveillance, a sousveiller A has fewer vulnerabilities to the other transaction participant B than if sousveillance is not employed. Then, for each prospective transaction[5] occurring between A and B, with A employing sousveillance, there are the following cases: (1) transactions that proceed (or not), but would have (not, resp.) proceeded anyway without sousveillance, i.e. A already trusts B; (2) transactions that proceed solely because of

[3]The canonical example is that of the pin makers given by Adam Smith [19]. He documents how a lone unskilled pin-maker might be pleased with an output of 1 pin per day, so that ten independent unskilled pin makers could produce 10 pins per day. However, by dividing the labor among the same ten men, each with a specialized task and station appropriate to the their task, one can expect a typical output of 48,000 pins per day, corresponding to an increase of $4800\times$ more pins per participant, using the same input materials and laborers.

[4]Hawala traders operate by accepting cash in local currency, then transmitting the payment order, along with a password, to another trader in the (generally foreign) destination city. The recipient can then pick up the money by presenting the password to the destination trader, usually the next day. The balance between traders is maintained informally, with no promissory instruments exchanged, so these transactions are based entirely on the honor system. Currency exchanges take place at market rates, rather than any official exchange rate. A typical commission fee is 0.2%-0.5%, which is far less than banks charge.

[5]We assume the "prospective transaction" is in good faith – both parties are voluntarily transacting and expect, ideally, to complete the transaction honestly. This rules out "transactions" such as theft, fraud, and "showrooming", i.e. examining merchandise without intention to purchase from that seller, only to purchase the same or similar product elsewhere.

sousveillance, and would not have without sousveillance, i.e. due to A's reduced vulnerabilities by employing sousveillance, mean that A has less reliance on trust and so is more willing to deal with party B; and (3) transactions that are aborted because of sousveillance – since our premise is that A employs sousveillance, this case indicates a rejection by B to engage in a transaction.

Now let us analyze these cases with respect to trust and transactions. In *case 1*, sousveillance has no impact on trust or transactions. In *case 2*, sousveillance allows transactions to proceed that would otherwise not be initiated, and so increases the number of transactions. This has the ancillary benefit of allowing a relationship to develop that may lead to the involved parties eventually trusting one another. In *case 3*, sousveillance has no impact on trust, and reduces transactions. While this appears to be an argument against sousveillance, it actually a direct validation of our thesis that societies that reject sousveillance will be impoverished, relative to those accepting sousveillance.

Therefore, sousveillance employed across many transactions (i.e. at a societal level) enables an increase in the volume of transactions, and so enabling greater specialization and consequently greater prosperity.

Since *case 3* illustrates the primary social issue blocking widespread use of sousveillance, as opposed to financial cost issues, or technological issues, let us examine this case in more detail. The refusal to deal in the presence of sousveillance implies a refusal to deal due to a change in the vulnerabilities of the involved parties. Namely, the one employing sousveillance is less vulnerable to the arbitrary authority of the other party, and the authority in fact may be made more vulnerable due to the ability of the sousveiller to obtain recourse from a more powerful entity such as a consumer advocacy bureau, the police, a judge, or public opinion.

One might make an argument based on emotion, that transactions may be aborted solely because the "feelings" of B, for example that A lacks sufficient trust and faith in B as evidenced by the choice to employ sousveillance. Thus, B is in fact reasoning about A's choice to engage in sousveillance.

Based on experience with the deployment of surveillance, feelings about sousveillance are a function of how often one encounters it. The present author finds widespread surveillance of roads, highways, offices, and shops highly disturbing, inducing a "creepy" feeling. However, with sufficient saturation of surveillance in society, it becomes merely another fact of life to which we adjust. In fact, in the case of the shop-keeper, we can empathize with their position in using technology to prevent theft and identify criminals. We also can recognize the benefit to all shoppers in the form of lower prices. Lastly, we recognize that while surveillance can easily be used as evidence against criminal acts, it is more difficult to use such recordings to implicate innocent individuals, and in fact may exonerate them from claims of wrong-doing.

B. Economic implications of information

We now consider transactions with respect to information available to transacting parties, and the effect of sousveillance in information asymmetries.

In "The Use of Knowledge in Society" [25], Hayek argues that the inherently decentralized nature of economic knowledge, specifically of prices, implies that the fundamental barrier to central economic planning is information. This means, for any real economy, the "price mechanism" summarizes the local information regarding cost, availability, and demand of any good, in such a way that others can reason about their economic decisions in a way that benefits all parties involved. Hayek was the first to clearly elucidate how the price mechanism leads to efficient allocation of resources, across society, by ameliorating the problem of local knowledge. The key insight is that on the whole, participants in any action have more information available to them than any central authority can possibly have. In general, limits of any central authority are cognitive in nature (although the specific bottleneck may be in data collection, collation, bandwidth, storage, processing power, or dissemination of results).

Economic information, i.e. information used in the decision-making process, does not only take the form of prices. For example, honest dealing, quality of service, prompt and complete fulfillment of explicit or implicit contracts, responses to exceptional conditions, and customer support, are all examples of non-price information that may have more influence on prospective buyers and sellers than price alone.

The branch of economics called *information economics*, or the *economics of information*, is concerned with the unique attributes of information when considered from an economic perspective [26], [27], [28, p. 20]. When one party to a transaction is in possession of relevant information not disclosed to the other party, this situation is referred to as an *information asymmetry*. In classical economics, *information* is typically considered in itself enough to enable a decision to be made – thus, if an economic actor (e.g. a consumer, manufacturer, insurer, etc.) is aware of a particular fact, then that information may be immediately used in their decision-making process.

In the context of an information asymmetry (i.e. where sousveillance is typically employed), however, raw information or knowledge of an event by an individual is often insufficient to obtain a desirable outcome. By definition, the sousveillance practitioner is not in a position of authority, and therefore, without verifiable documentary evidence, information reported by the sousveiller to any higher authority may be on its own insufficient to attain their goal and to meet the *needs* of the sousveiller. Testimony can be challenged by other testimony,[6] and in this situation, the person with greater

[6]Former San Francisco police commissioner Peter Keane, in a 2011-Mar-15 *San Francisco Chronicle* article "Why cops lie", comments: "Police officer perjury in court to justify illegal dope searches is commonplace. One of the dirty little not-so-secret secrets of the criminal justice system is undercover narcotics officers intentionally lying under oath. It is a perversion of the American justice system that strikes directly at the rule of law. Yet it is the routine way of doing business in courtrooms everywhere in America."

authority has an advantage.[7]

For available information to be acted upon, whether by a consumer making a purchase or a judge making a ruling, the quality of any information is critical in determining to what degree it affects any decision regarding how to act. Veracity and accuracy cannot always be determined by testimony alone, and when conflicting testimony is presented, often the participant in a position of authority is more trusted. However, if information is timely, organized, and presented with supporting evidence, then the determination of veracity depends less upon the authority of the one testifying.

By the nature of authority there are, in general, fewer parties in authority, than the number of parties not in authority. This is true because if more than one party wishes to enforce their will, conflict arises, and by definition the party with greater ability and (normative) legitimacy becomes the one in a position of authority. Therefore, using definitions from Sec. I-C, surveillance in a transaction is inherently monopolized by the party in a position of authority (and those in authority over them, who are in general outside the transaction). Sousveillance, on the other hand, is inherently *distributed* in nature. Sousveillance enables real-world events to be captured from multiple perspectives and from multiple parties' points-of-view, rather than only from a central (panoptic) perspective.

Let us examine two specific examples of dilemmas of information asymmetry, and how sousveillance can be used to help resolve them.

1) Adverse selection, or inability to know behavior pre-transaction: Adverse selection occurs when a transaction is constructed with the parties having an information asymmetry, and the outcome of their negotiation, e.g. cost or willingness to engage at all, substantially differs from what would occur under the condition of perfect information where all parties share all information and act accordingly.

There are two usual strategies [29] for combating adverse selection. One is *screening*, used by the less-informed party when they must initiate the transaction. An example of screening is qualifying customers for a bank loan. The other usual strategy is *signalling*, generally used by the more-informed party. A job-seeker conveying to a potential employer their educational credentials is a canonical example of signalling.

Sousveillance forms an interesting point in this dilemma, since it can act in both roles, to screen and to signal. Consider a retail shop as being the informed party, and say that they allow sousveillance to be used on their premises to *signal* to prospective customers that they are willing to have their customer interactions on record. This works to alleviate apprehension that potential customers may have in doing business with them. Likewise, conspicuous use of sousveillance by a potential customer can serve to *screen* businesses that are not willing to do so.

[7]Furthering the argument, in a 2013-Feb-02 *New York Times* article "Why Police Lie Under Oath", Michelle Alexander describes some of the perverse economic incentives that lead to these counter-productive practices, such as illegal quotas for the number of arrests police need, to obtain associated rewards, combined with a lack of consequences for professional misconduct.

2) Moral hazard, or inability to know behavior post-transaction: This dilemma occurs when an information asymmetry induces one party A to assume a risk, that another party B is obliged to pay for. The canonical example is in insurance, where an insured party has complete knowledge of their own risk-taking behavior, but the insuring party can only infer from past records as to the level of risk. While every case of moral hazard involves some degree of adverse selection, adverse selection can occur on its own, with any good that can only be fully judged after being bought and used.

Sousveillance can play a valuable role in lessening the problem posed by this dilemma, by enabling a reduction in the information asymmetry. For example, a contractor working in a high-risk environment may opt to use sousveillance to reduce his occupational hazard insurance premium. Likewise, a driver may choose to record his own actions to obtain a lower premium on his car insurance.[8]

C. Opportunism

Opportunism is the taking of unfair advantage of another party. Combating opportunism is arguably the most important factor [30, p. xi] in establishing economic prosperity, at both the micro and macro scales. For opportunism to occur, there typically must be an imbalance in either knowledge or power between the transacting parties. A "golden opportunity" [31] is a situation in which a party can engage in opportunistic behavior without any possibility of getting caught. By reducing exposure to such "golden opportunities", sousveillance acts to reduce the "attack surface" of potential victims. Some forms of opportunism have already been discussed, for example moral hazard can be considered a form of reneging on a contract. In [30, pp. 30–36] Rose proposes a classification of the different kinds of opportunism into three degrees, which we present here with an examination of the roles sousveillance plays in combatting them.

1) First-degree opportunism: This "involves taking advantage of the imperfect enforceability of contracts". Examples include reneging on contracts, shirking, and self-dealing. These practices are typically illegal, and so can be legally remediated, if caught. Sousveillance has immediate and obvious applicability to this situation in two respects.

One way sousveillance applies is that enforcement of contracts requires information regarding the execution of the contracted good or service. By engaging in sousveillance, the party executing the contract can verifiably demonstrate that the agreed-upon terms are being met. To give a simple example, consider hiring a house painter, who agrees to sand and clean all surfaces, apply primer, and use three coats of top paint. After the job is completed, it may be difficult for the customer to determine if the correct and agreed-upon process was followed, or if the painter was shirking his contractual obligations. Using sousveillance, the painter can generate hard

[8]Note that if there is no other option available, e.g. having insurance is mandatory, and recordings are mandatory, perhaps because there is only one insurance company in that field, and the recordings are sent directly to them, this becomes surveillance.

evidence that the contract was fulfilled correctly.[9] In this way, sousveillers can mitigate accusations and suspicions of first-degree opportunism.

The other obvious way that sousveillance applies to first-degree opportunism is in the detection of it, and in the identification of the culprits. For example, consider a theft of personal property occurring in a busy and crowded area, with heavy surveillance, such as at a cafe in a shopping complex at lunchtime. Obtaining surveillance recordings is at the discretion of the property managers, and even if available, are likely to cover such a wide field-of-view that the perpetrator may not be identifiable. Sousveillance affords a first-person perspective covering the immediate vicinity of the sousveiller, is immediately available for review and, if necessary, available for submission to either the authorities for investigation, or to appeal to the public for further information about the offender. In this way, sousveillance acts as a mechanism to reduce the cost of justice, since obtaining forensic evidence becomes routine and inexpensive.

2) Second-degree opportunism: This form of opportunism "involves taking advantage of the incompleteness of contracts because most contracts cannot anticipate every possible eventuality". This form of opportunism is typically legal, so the usual remedy is to cease dealing with the offending party. Routine examples of incomplete contracts are those for employment, which may execute over years or decades. Contracts of any significant duration are generally incomplete, since as Klein [32] notes:

> *"When a large number of possible contingencies exist regarding future events, the use of the fully contingent complete contract of economic theory is too costly. Transactors use incomplete contracts in these circumstances not only to avoid the significant « ink costs » of writing fully contingent contracts, but, more importantly, because incomplete contracts avoid the wasteful search and negotiation costs that otherwise would be borne by transactors... Transactors enter relationships knowing they have left some unlikely contingencies unspecified, recognizing that if such a contingency develops, it will have to be handled after the fact. In addition to avoiding the rent dissipating search and negotiation costs involved in complete contractual specification, contracts are incomplete because of measurement costs."*

Sousveillance can help combat second-degree opportunism in two ways. One is that because it allows the negotiation process to be on record, at very little cost, this gives the transacting parties a basis to reason about the implicit understandings in a contract. With sufficient timestamping for sequencing negotiations, so that later clarifications are accounted for, it is reasonable to expect that any dispute arbiter would accept a sousveillance-based record of negotiation as definitive for determining the interpretation of what was actually agreed to in a contract.

A second way that sousveillance can help is that it enables certain measurements to be routine and inexpensive. In the case of video sousveillance, these are measurements based on visual inspection. This implies that at least some measurement of the executing process can be stated explicitly in contract, thus avoiding incomplete contract specification due to concern about measurement cost, in the applicable domain.

3) Third-degree opportunism: Finally, third-degree opportunism "involves taking advantage of discretion that exists in a relational contract". A "relational contract" is one in which the explicit terms are very broad, relying heavily on implicit understandings and the discretion of the parties involved. The prototypical situation is that a principal hires an agent to perform some specialized function (e.g. a doctor, lawyer, engineer, or CEO). In the course of carrying out his duties, the agent decides to accept a lower payoff for the principal in exchange for a higher payoff for himself. Then we say that the agent has engaged in third-degree opportunism.

For example, say an unknowledgeable car driver (the principal) takes their vehicle for repair into an auto shop. The mechanic (the agent) then examines the vehicle for problems, and makes his recommendations for repairs. The principal has no way to immediately evaluate the veracity of the agent's recommendations, and is therefore vulnerable to third-degree opportunism.

In this case, sousveillance can be employed in a similar manner as in first-degree opportunism, but by the principal rather than the agent. In our example, the car owner can convey detailed information of the interaction to another mechanic or other knowledgeable person either at the time of the transaction, or after it is completed, to determine if the mechanic was in fact behaving opportunistically.

4) Sousveillance and the Degrees of Opportunism: In all three degrees of opportunism, sousveillance affords some mechanism for combatting the behavior, and in the other direction, can often help a wrongly-accused party to establish their innocence. Of course, sousveillance cannot address all instances of opportunistic behavior, since the root cause is internal to the decision-making process of the offender. The basic mechanism that is common to all cases where sousveillance can be applied, ultimately, is that sousveillance enables accountability. The path to this desirable outcome may take the form of detecting opportunism, identifying the persons responsible for it, or dispelling accusations of opportunism.[10]

[9] Sousveillance may incidentally provide other benefits for a sousveiller. Consider the following advertisement.

> Who would you rather hire to paint your house? Us, who offer a sousveillance video of the process, or our competitors, who don't?

[10] Accountability for actions implies both negative consequences (punishments) and positive ones (rewards). Sousveillance functions in the same way with respect to laudable moral behaviors, as with reprehensible ones. Thus, by using sousveillance to detect laudable behaviors, and identifying the persons responsible for them, sousveillance also allows those responsible to be rewarded.

D. Bureaucratic terror and sousveillance

The preceding sections of the present work have dealt primarily with voluntary economic transactions that are financial in nature. In this section, however, we consider sousveillance as a mechanism for avoiding undesirable feelings when dealing with bureaucrats, such as helplessness, powerlessness, and ultimately, terror. These transactions may be compelled by legislation, and therefore, as non-voluntary transactions, take on different characteristics than those based on voluntary good faith. In particular, the asymmetries in both authority and information are generally more extreme, and the option to "vote with one's feet" and find another service provider isn't available, in general, when transacting with a bureaucracy.

The word "bureaucracy" comes from the French for desk or office, "*bureau*", and the Greek for political power, "$\kappa\rho\acute{\alpha}\tau o\varsigma$" or "kratos" in the Latin alphabet. Terror, from the Latin for "great fear", is an emotional state of extreme fear. Fear, in general, is a healthy reaction to potential sources of risk. For example, a person may reasonably feel fear when standing near the edge of a high cliff, or when working with a hot stove. Fear acts to help preserve bodily integrity and well-being. When the degree of fear becomes too intense, rather than having a protective function, it leads to paralysis, irrational behavior, and even lashing out. Therefore, let us recognize terror as a kind of unhealthy fear. An *inconsistent* and *disproportionate* response from an external interaction can induce this state, even in a healthy person [33, Ch. 1].

1) Bureaucracy: The modern bureaucratic system of administration was championed by writers on management such as Weber, Taylor, and Drucker. One of the key benefits of a bureaucracy, as envisioned by Weber,[11] is that rules are applied impersonally; treatment of each transaction depends only on the criteria strictly relevant to the situation at hand, e.g. not based on personal whims, patronage, nepotism, or other arbitrary criteria. However, as noted by Mises [35],

> "The terms *bureaucrat*, *bureaucratic*, and *bureaucracy* are clearly invectives. Nobody calls himself a bureaucrat or his own methods of management bureaucratic. These words are always applied with an opprobrious connotation. They always imply a disparaging criticism of persons, institutions, or procedures."

He goes on to point out that bureaucracies in the private sector are invariably developed as a consequence of government-granted monopolistic rights, since otherwise there are always alternatives for customers to turn to, forming a natural antidote to bureaucracy. In this section, we specifically examine non-consensual bureaucratic transactions, i.e. with a government bureaucracy – for example, a City Hall, the police, emergency first-responders, courts, or any of the multitude of Administrations, Departments and Ministries of modern nation-states.

2) Depictions of Bureaucracy: Bureaucratic terror is a staple of dystopian novels, such as Franz Kafka's "The Trial" (1925) and "The Castle" (1922), and Yevgeny Zamyatin's "We" (1924). Other fictional depictions include Bulgakov's "The Master and Margarita" (1967) and C.S.Lewis' "The Screwtape Letters" (1942). A typical description from this genre, from the preface to "The Screwtape Letters", runs as follows.

> *"I live in the Managerial Age, in a world of "Admin." The greatest evil is not now done in those sordid "dens of crime" that Dickens loved to paint. It is not done even in concentration camps and labour camps. In those we see its final result. But it is conceived and ordered (moved, seconded, carried, and minuted) in clean, carpeted, warmed and well-lighted offices, by quiet men with white collars and cut fingernails and smooth-shaven cheeks who do not need to raise their voices. Hence, naturally enough, my symbol for Hell is something like the bureaucracy of a police state or the office of a thoroughly nasty business concern."*

3) Cognitive Limits of Bureaucracy: Even with the best of intentions, bureaucracies in welfare states face the same kind of cognitive barriers that Hayek illustrated with respect to pricing, discussed above in Sec. II-B. As Wagner [36, p. 20] states:

> *"Expositions of welfare economics typically assume that the analyst possesses knowledge that is in no one's capacity to possess. A well-intentioned administrator of a corrective state would face a vexing problem because the knowledge he would need to act responsibly and effectively does not exist in any one place, but rather is divided and dispersed among market participants. Such an administrator would seek to achieve patterns of resource utilization that would reflect trades that people would have made had they been able to do so, but by assumption were prevented from making because transaction costs were too high in various ways. A corrective state that would be guided by the principles and formulations of welfare economics would be a state whose duties would exceed its cognitive capacities."*

This means that regardless of the intentions of the bureaucrats, when resource allocations, or higher-order means controlling them, are centralized, then mis-allocation is bound to occur. The issue is fundamental and cognitive in nature, and so while measures may be taken to improve the situation (i.e. make it "not worse") it appears that it is impossible to make the mis-allocation disappear (i.e. make the situation "better").

4) Bureaucracy and Power: Bureaucrats have the legal force of their respective governments backing them. This is not quite the same as having power over their euphemistically-named "customers" – those who must contend with the bureaucracy. In "On Violence" by Hannah Arendt [37, p. 239], she delineates "power" as the ability to voluntarily regulate, control, and make decisions in a social context. On the other hand, "violence" indicates a lack of power, and forms a means to gain some of the characteristics of power, and in this way, violence acts as a kind of simulacrum of genuine power. That

[11] In [34, pp. 956–958], Weber enumerates his six bureaucratic characteristics as: imperial positions, rule-governed decision making, professionalism, chain of command, defined responsibilities, and bounded authority.

is to say, while some "customers" accept the legitimacy of the bureaucracy, and therefore the bureaucracy holds genuine power over them, in other cases the "customer" transacts with the bureaucracy only due to the implicit threat of violence. While in general one may see a bureaucracy as simply an administrative function, insofar as "[a] durable system of government must rest upon an ideology acknowledged by the majority" [17, p. 189], the "customer" is aware at some level that ultimately, every government bureaucracy has recourse to violence, to force acquiescence to their rules.

Those rules are generally in accordance with the public legal code, usually published in a set books, such as the "Code of Federal Regulations" in the USA. However, the actual operation of administrative functions relies on a set of handbooks and guidelines commissioned and published by the bureaucrats themselves. Let us refer to these as the "*second set of books*" [38]. Without direct access to the "second set of books", the "customer" has no way of reliably knowing what the outcome of a bureaucratic process will be. This uncertainty creates fear in the "customer". Depending on the degree of not knowing what to expect (i.e. the "customer" knowing only that they may suffer disproportionate or inconsistent responses, backed by the force of law), this fear can pass beyond the point of "healthy fear" and into the domain of terror.

5) Sousveillance in Bureaucratic Transactions: Sousveillance acts toward alleviating the asymmetry in information and authority inherent in a bureaucratic transaction. One way this occurs, with respect to authority, is that the "customer" is able to share his side of the story, with full documentary *evidence* rather than mere *testimony*. This is true for both a bureaucratic transaction itself, and for any events leading to the bureaucratic transaction. Sousveillance allows a sousveiller to share the context of potentially controversial actions, so that both bureaucrats and the public can review the evidence from a first-person perspective.

If a transaction proceeds with a poor outcome, the "customer" may then appeal to higher authorities or the public. Sousveillance functions to provide the sousveiller, who by definition lacks authority in dealing with the bureaucracy, with a simulacrum of authority (see also "swollag"[12] in [39]). This reduces the terror in the "customer", since as a sousveiller the "customer" has evidence to challenge disproportionate bureaucratic responses so that they may not need to suffer them. Another way that sousveillance can improve the situation (i.e. transactional outcome) is with respect to information. As sousveillance becomes more widespread, more recordings of bureaucratic interactions become available for review. Armed with instructional sousveillance video of previous transactions, "customers" can know better what to expect, and are better able to identify inconsistent behavior from the bureaucracy.

In the present work, we focus on video sousveillance for clarity; however, USA's federal *Freedom Of Information Act* (FOIA) enables a kind of sousveillance where the artifact produced is a literal copy of "the second set of books", as well as related case-specific information. These forms of cooperative sousveillance (*"Access to Information"* acts) have been implemented, in various forms, by many nations (e.g. Canada, France, Norway) as well as many state and provincial legislatures. When successful, this form sousveillance can clearly reduce the information asymmetry between a bureaucracy and its "customer". This gives insight into the bureaucracy's operation so that the "customer" can successfully reason about what reactions to expect. We predict FOIA-type laws will continue to spread, since as a form of sousveillance they also give rise to economic efficiency in non-voluntary transactions.

[12]Swollag is to the authorities, what gallows are to the commoners. Swollag is also gallows spelled in reverse.

E. Summary of Economic Benefits of Sousveillance

Sousveillance can:

- reduce the cost of justice, per Sec. II-C1,
- reduce a sousveiller's vulnerabilities to other transaction participants, per Sec. II-A,
- reduce transaction costs by limiting "golden opportunities" for opportunism, per Sec. II-C,
- enable transactions that otherwise would not occur, per Sec. II-A,
- provide context for controversial actions, per Sec. II-D5,
- reduce information asymmetry, per Secs. II-B, II-D5,
- discourage negative outcomes and encourage positive ones, per Sec. II-C1,
- enable accountability, per Sec. II-C4, and
- be shown to be inherently distributed, per Sec. II-B.

III. Morality and Sousveillance

In this section we briefly review some general properties of morality, and apply these properties to two kinds of action, namely *sousveillance*, and *forbidding sousveillance*. We show that while sousveillance is a descriptive term, not a normative one, the act of *forbidding sousveillance* may prevent positive moral actions to be taken.

A. Positive and negative moral actions

In general, classes of human action (i.e. verbs) when considered without context, are *amoral*; this means that mere *descriptive terms* regarding actions are morally neutral. Morality does not exist in the kind of action itself, which is merely a tool to accomplish an end, and the morality of any particular action can only be rationally considered in-context.

Certain terms used to indicate actions are morally lauded or proscribed in the very definition of the word, such as theft or murder. Thus, these terms for actions are morally normative, in that their application intrinsically praises or condemns persons engaged in those actions. Morally normative terms form an exception to the general rule of human actions being amoral absent context. Consider the moral prohibition: "do not steal". This indicates that the action indicated simply should not be performed, at all. If the prohibited activity is engaged in, it requires a strong explanation. Conversely, consider the moral exhortation: "be charitable". The exhortation indicates a moral benefit from being charitable, that is, this action should be

engaged in when possible – it is not a commandment that this action needs to be carried out at all time (e.g. in lieu of feeding one's family).[13]

Moral value judgments of positive moral actions can serve two distinct purposes: one purpose is to help decide which of the many potential positive moral actions available to an individual should be carried out,[14] and another is to evaluate the degree of success within a particular kind of action.

In [30], Rose argues that any economically successful system of morality must consider negative moral actions universally, from a non-consequentialist perspective (i.e. do no wrong, regardless of the consequences[15]), whereas positive moral actions must be considered from a consequentialist basis (i.e. each potential action is evaluated by its consequences) in order to select which actions to take. Accepting this foundation implies that we then have a rational basis to determine both the *form* or kind of positive moral action, by using consequentialist reasoning to compare multiple alternatives, and to determine to what *degree* should we engage in that positive moral action, again using consequentialism to maximize benefits and minimize costs.

Another point that helps to see the asymmetry between positive and negative moral actions, is that positive moral attributes are often defined as optimums between negative moral attributes – but not the reverse. For example as noted in [8], Aristotle pointed out that "courage" is the optimal balance between recklessness and cowardice, and likewise "generosity" can be considered the optimal balance between stinginess and profligacy. In this way, we can see why for any particular positive moral action, it is impossible to have *too much* of it, considered by itself – only relative to other potential positive moral actions can such a decision be made.

B. Application to Sousveillance

Having distinguished between the moral values regarding positive moral actions and negative moral actions, an important issue is whether a positive moral action can depend on sousveillance; if so, then an absolute prohibition of sousveillance forms a negative moral action in itself. To establish the non-normative property of sousveillance, let us consider a particular case.

A man engages in sousveillance, and thereby obtains documentary evidence regarding the commission of a crime. Now, with this information, the sousveiller has multiple options, including doing nothing. Other options are presenting the evidence to the victim, the public, or to legal authorities. These latter actions may help bring the perpetrator to justice, and therefore the complete set of actions can be considered morally laudable. Note that the sousveillance itself is seen as neither a positive nor negative moral action, although it enables a positive moral outcome, namely justice.

However, the sousveiller has still other options, including presenting the information to the criminal in an effort to commit extortion.[16] Now, the same information is used in the commission of a new crime. Since extortion is normatively a negative moral action, any moral code abiding by the moral foundation [30] must clearly distinguish which actions are negative in a binary sense.

We conclude, given that the sousveiller had the option of furthering justice but instead may choose to further an illegitimate self-interest, that the sousveillance itself is neither grounds for praise nor for condemnation. Therefore, in our hypothetical example, sousveillance is merely descriptive of an action.

Since considering an action as a normative action by definition must apply in general, in that they function to establish *norms* of behavior, and because the normative label doesn't apply in this case, then we have established that sousveillance is merely descriptive of an action, and is not a normative term in general. We have also given a concrete example of how preventing the use of sousveillance may frustrate justice; in particular, if a sousveillance record of an event is the *only* documentary record that can be submitted for scrutiny.

IV. The Rise of Sousveillance

A. Technological Trends

In the case of sousveillance we have outlined in previous sections why, at a micro scale, sousveillance as a practice makes economic sense. But, we have ignored the technological basis for sousveillance, as well as the conditions for widespread acceptance of sousveillance.

From a technological perspective, the basic elements required for wide-scale sousveillance are in place, although not in our preferred embodiment based on HI. High-speed wireless networks are commonplace, as are small form-factor devices (e.g. smartphones) capable of being worn in regular clothing and capable of recording and transmitting video and audio recordings wirelessly. At present, always-on active transmission of video is limited by the size of portable energy supplies. However, such technology is constantly improving in multiple ways, including user interface, camera resolution, network bandwidth, and pecuniary cost of hardware and service.

Therefore, if present technological and commercial trends continue, we expect that effective video sousveillance equipment will soon be available to anyone who can currently afford a mobile phone; and, as costs come down, this proportion of the population will only grow.

[13]Theft may be considered morally acceptable to feed one's family as a one-time event to preserve life, however, this is an example of an exception with justification. Routine theft, even to feed one's family, ultimately leads to impoverishment on a larger scale for both sellers who must charge more and invest in security, and all other consumers, who must pay more.

[14]For example, a person helping another may need to decide, *should I give this person money, or instead provide encouragement and assistance in gaining employment?* Positive moral actions in general require resources which are finite, such as money and time.

[15]Exceptions can be made, however, they must be specific in nature and not merely appeal to a "greater good" rationalization. See [30, ch. 6-8] for details.

[16]The best weapon against extortion may be sousveillance; in a sousveillance society (i.e. where sousveillance is widespread), extortion will tend to be discouraged or at least brought to justice in many situations, especially if both parties are conducting sousveillance.

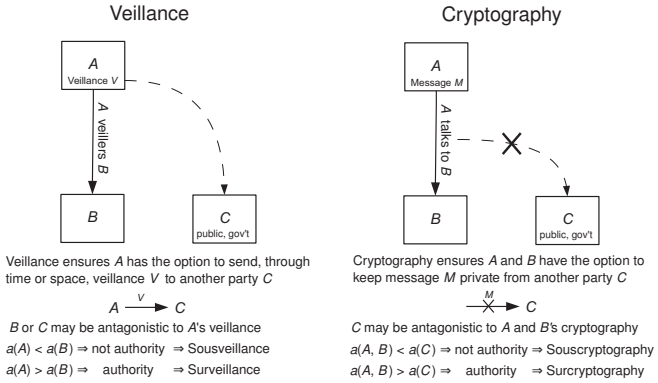

Fig. 3: System diagram of veillance and cryptography, where: a = authority function, A = primary participant, B = second participant, C = external party, M = message, and V = veillance. In contrast to cryptography, within a transaction between parties A and B, sousveillance does not require A and B to cooperate. Party C is outside the transaction, and may be the public, a friend of A or B, or a legal authority such as a court. Both kinds of action (veillance and cryptography) enable control of information within the transaction, veillance by allowing it to be shared, and cryptography by allowing it to be private.

B. The analogy between cryptography and veillance

In Sec. II-A, we briefly considered the social acceptance of sousveillance based on experience with widespread surveillance. However, there is a key and fundamental difference between sousveillance and surveillance: surveillance by definition is reserved for those with authority, whereas sousveillance is not. Since those persons with authority are the ones who, in practice, determine the rules that those without authority submit to, such comparisons between sousveillance and surveillance are limited in their generality. Another approach is required to model this critical aspect of sousveillance.

There is a natural analogy between veillance and cryptography, as shown in Fig. 3. Cryptography, like veillance, may be distinguished by the domain of application, and takes on different characteristics depending on the authority relationships between various parties.

Let us consider an individual as being capable of *action*, and an action involving multiple persons, called the *participants*, as a *transaction*. Now consider a party external to a particular transaction (a *third party*). Both cryptography and veillance then act to control (restrict or enable dissemination of) information about the transaction.

In commerce, we wish to minimize transaction costs. In the domain of online sales, cryptography contributes to this goal by keeping sensitive payment information out of view from criminals that may wish to use those payment details for their own purchases. Likewise, if an employee wishes to share confidential business plans with a colleague online, encryption is typically used (e.g. a corporate VPN) to again prevent the dissemination of the confidential information – say from their competitors – again contributing to efficiency thereby reducing transaction costs and increasing prosperity.

However, as these two examples of cryptography illustrate, the participants in a cryptography-based transaction must cooperate to accomplish their transaction. If either party is antagonistic to the use of cryptography, then the transaction either doesn't proceed, or proceeds by other means.

Yet, historically we see examples of antagonists to cryptography, using their authority to mandate controls on the use of it. There is a very clearly analogous situation, as in sousveillance. Referring again to Fig. 3, we see that when parties in positions of authority engage in cryptography (we can refer to this as *surcryptography*), but at the same time prevent others from using it (i.e. engaging in souscryptography), then the present dynamic of "McVeillance" (surveillance, combined with a prohibition on sousveillance) [40] is replicated in the domain of cryptography, forming a system of "McCryptography".

McCryptography was in fact the usual state of affairs, until two key events occurred. One was the release of PGP, in particular its source code; and the second event was the creation of the World-wide-web, composed of servers and clients using the HTTP protocol and graphical user interfaces. The first event provided the technological capability, and the second created the economic necessity of cryptography being available for personal use.

1) The legal status of PGP: While governments and large corporations have had access to strong cryptography at least since 1982, when RSA Inc. (now a part of EMC Corp.) made their products available on the market. Later, in 1991, Phil Zimmerman released the first version of PGP, including the source code which was subsequently uploaded to the Usenet message system. The well-known cryptographer Bruce Schneier considered PGP as "the closest you're likely to get to military-grade encryption." [41, p. 587]. Usenet by design replicates posts across its global network, so that political dissidents, cypherpunks (free communication activists), peace activists, criminals, and ordinary citizens around the world now had access to cryptography strong enough that it was in practice unbreakable by any adversary, including governments.

Soon after the release of PGP, in February 1993, the author Phil Zimmerman became the target of a federal criminal investigation, and was charged with "exporting munitions without a license" [42, pp. 368–370]. The law current at the time considered encryption software using keys greater than 40 bits in length as "munitions", so the 128-bit scheme used in PGP was classified as such. Zimmerman reacted by reasoning that while software could be classified as munitions (along with firearms and missiles), it had already been legally established that books were protected as free speech. So, he published his source code in the form of a printed book. The case was dropped, so his theory was never tested in court.

2) The Liberalization of Cryptography: Citing economic concerns, the legal control regimes around cryptography were substantially liberalized [43, p. 2.118], not just in USA, but in most of the world, with the exception of France. Even in France, exceptions have been made for precisely the reason we argue that widespread sousveillance is inevitable: economic prosperity. Secure online banking and online shopping for goods and services are "killer apps" for cryptography. No government wishes to drain their coffers by prohibiting technological developments, when they have the potential to dramatically improve economic efficiency. Numerous large

corporations have indeed sprung up around cryptography and data security, far more so than would supported by a purely "crypto-as-munitions" legal regime.[17]

Important new use cases (since the mid-1990's) for cryptography have become routine: VPNs for remote network access to corporate data, whole-disk encryption, secure single-sign-on across a large range of Internet properties from providers such as Google, Yahoo!, and Microsoft, and whole-system cryptography for "cloud computing" encompassing both disk images and all network communications, are a few among the many novel uses of cryptography.

This sequence of events does not imply that the liberalization of cryptography happened automatically, without any conscious thought or effort. On the contrary, there were extensive efforts from advocates, activists, and researchers to educate businesses, the public, and legislators of the importance of cryptography. For example, here are a couple of examples of typical arguments for a liberal cryptography regime, from the early 1990's.

> *"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds."* – John Perry Barlow [46].
>
> *"I want a guarantee – with physics and mathematics, not laws – that we can give ourselves real privacy of personal communications."* – John Gilmore, [47].

These quotes are from the early days of the "cypherpunk" movement, when the arguments were more about ideals, rather than economic necessity. Since thought is the hallmark of human action, and thoughts are directed by ideals, the fundamental "rightness" of ordinary people having access to strong cryptography was a necessary precursor to the economic argument.

3) Implications for Sousveillance: In our analogy, cryptography is a kind of inverse of veillance. Both enable control over the information in a transaction, cryptography by giving the option to keep it private, and veillance by giving the option to share it. Referring back to our original definition in Sec. I-C, the key property of veillance is that it produces an artifact that can be moved through time or space.

Sousveillance, like souscryptography, has to date encountered substantial resistance from those in positions of authority. Like souscryptography, as the availability of and economic reliance on sousveillance increases, we expect that economic self-interest will compel those in positions of authority to re-consider their antagonism to sousveillance in light of self-interest, and ultimately self-preservation. As with souscryptography, antagonism towards sousveillance may initially confound using it routinely. However, the increases in economic efficiency, personal safety, and accountability that sousveillance affords are of a like scale, as those afforded by souscryptography.

[17]Strong cryptography is still considered a munition in USA. However, it is reportedly straightforward now for companies to obtain an export license [44], although the cost of $250 per license may be prohibitive for Free Software [45] projects and the like.

Therefore, we expect a similar development and deployment path for sousveillance as with souscryptography, with initial resistance but later acceptance, once the overall benefit to all parties is evident. As we've seen with souscryptography, this process is not automatic, and requires strong advocates and practitioners to make those benefits evident to the involved parties, and to create a sustainable industry supporting sousveillance.

C. Thought Experiment

Consider two contemporaneous societies. One is pro-sousveillance, A, the other is anti-sousveillance, B. In both A and B, we assume surveillance is at least as common as we see today. And, assuming present technological trends continue with respect to hardware and networking, the technical ability to engage in sousveillance in this scenario comes at a cost comparable to present-day mobile phone use, and therefore is potentially ubiquitous.

In A, we see retail businesses that allow routine sousveillance by customers, enabling easier price comparison and greater personal safety. We also see a range of service-providers that agree to engage in sousveillance so that customers can routinely verify that work was done to the agreed-upon standard. Interactions with representatives of government institutions, such as emergency first-responders, licensing and passport offices, courts, and so on are routinely recorded by their "customers", to reward those responsible for positive outcomes, and provide feedback to the administration regarding negative ones. The cost of justice is lower than in B, so that bringing opportunists to justice is more likely, and furthermore, those wrongly accused have a documentary evidence with which to defend themselves.

Now in B, where we have a regime similar to that in place today, engaging in sousveillance is technically as straightforward as in A, but the social and legal recognition of the value of sousveillance has not taken place.

Then the key question is, will the people of A move towards B's position regarding veillance, or will the people of B move toward A's?

If concerns of privacy come to dominate the discourse, than we would expect surveillance in B to be scaled back, perhaps proportional to the degree of sousveillance possible (which, since we assume B is anti-sousveillance, is close to none at all). Since sousveillance by its nature is most beneficial to those who otherwise lack authority, and provides them with a means of recourse in any dispute, it therefore can appeal to the bulk of society, not just those in positions of authority. However, the genuine economic benefits go to all parties, not merely the ones at the top or bottom of any hierarchy. This means B moves from McVeillance, i.e. surveillance but little sousveillance, to one of equiveillance, where the degree of surveillance is approximately equal to that of sousveillance, even if both are minimal. However, since in reality powerful interests have successfully introduced surveillance, and the practice is entrenched, we see this as

unlikely to dissipate. Therefore, B approaches a non-negligible state of equiveillance, which is the state of A.

Thus we conclude that people in B, having observed the economic efficiency, personal safety, fairness, and ultimately, the accountability afforded by sousveillance, will move toward adopting the policies of A regarding sousveillance.

V. Conclusion

In this work, we have considered the use of sousveillance from an economic perspective. We have enumerated properties of sousveillance with respect to economic transactions. In particular, how sousveillance can reduce asymmetries in information, and how sousveillance can be used to reduce economic opportunism occurring in varying degrees: in the imperfect enforcement of contracts (first degree), with incomplete contracts (second degree), and in the principal-agent problem (third degree). We also discuss bureaucratic (non-voluntary) transactions, and how sousveillance can be used in an institutional setting to promote accountability and positive outcomes. Finally, we consider the development and deployment of sousveillance as analogous to the use of personal cryptography, and argue that similar economic pressures will compel the acceptance of sousveillance. We explore this line of thinking in a thought experiment, and conclude that if social and technological trends in place today continue, the widespread and routine use of sousveillance is inevitable.

References

[1] dictionary.com. Online etymology dictionary. *Dictionary.com Unabridged*, 2010.

[2] S. Mann, J. Nolan, and B. Wellman. Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, 1(3):331–355, 2002.

[3] G. Fletcher, M. Griffiths, and M. Kutar. A day in the digital life: a preliminary sousveillance study. *SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1923629*, September 7, 2011.

[4] K. Michael and MG Michael. Sousveillance and point of view technologies in law enforcement: An overview. *IEEE Technology and Society Magazine*, 2012.

[5] J. Bradwell and K. Michael. Security workshop brings' sousveillance'under the microscope. *News @ University of Wollongong*, 2012.

[6] C. Reynolds. Negative sousveillance. *First International Conference of the International Association for Computing and Philosophy (IACAP11)*, pages 306 – 309, July 4 - 6, 2011, Aarhus, Denmark.

[7] V. Bakir. *Sousveillance, media and strategic political communication: Iraq, USA, UK*. Continuum, 2010.

[8] S. Banerjee, N.E. Bowie, and C. Pavone. An ethical analysis of the trust relationship. In R. Bachmann and A. Zaheer, editors, *Handbook Of Trust Research*, pages 303–317. Edward Elgar Publ., Cheltenham UK, 2006.

[9] Edward J. Hackett, editor. *The handbook of science and technology studies*. The MIT Press, Cambridge, 2008.

[10] F.C. Brentano and C. Hague. *The origin of the knowledge of right and wrong*. ATLA monograph preservation program. Archibald Constable, 1902.

[11] F. Brentano. *Psychology from an Empirical Standpoint*. International Library of Philosophy. Taylor & Francis, 2009 [1874]. Translation to English by Routledge, 1995.

[12] John R. Commons. Institutional economics. *History of Economic Thought Articles*, 21:648–657, 1931.

[13] R.H. Coase. The nature of the firm. *Economica*, 4(16):pp. 386–405, 1937.

[14] Oliver E. Williamson. Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics*, 22(2):pp. 233–261, 1979.

[15] O.E. Williamson. *The Mechanisms of Governance*. Oxford University Press, USA, 1996.

[16] Steve Mann. Wearable computing: Toward humanistic intelligence. *IEEE Intelligent Systems*, 16(3):10–15, May/June 2001.

[17] Ludwig von Mises. *Human Action: A Treatise on Economics*. Ludwig von Mises Institute, 2010 [1949].

[18] Plato. *The Republic (Penguin Classics)*. Penguin Classics, 1955.

[19] A. Smith. *Wealth of Nations*. Penguin classics. Penguin Group, 1999 [1776].

[20] D. Ricardo. *On the principles of political economy, and taxation*. John Murray, 1821.

[21] Matthias Schramm and Markus Taube. Evolution and institutional foundation of the hawala financial system. *International Review of Financial Analysis*, 12(4):405 – 420, 2003. Special issue: alternative perspectives in finance.

[22] M.E. Qorchi, S.M. Maimbo, J.F. Wilson, and IMF. *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*. Occasional Paper. International Monetary Fund, 2003.

[23] Nikos Passas. Fighting terror with error: the counter-productive regulation of informal value transfers. *Crime, Law and Social Change*, 45:315–336, 2006.

[24] Avner Greif. Contract enforceability and economic institutions in early trade: the maghribi traders' coalition. *American Economic Review*, 83(3):525–48, June 1993.

[25] Friedrich A. von Hayek. The use of knowledge in society. *American Economic Review*, 35:519–530, 1945.

[26] B. Allen. Information as an economic commodity. *The American Economic Review*, 80(2):pp. 268–273, 1990.

[27] Economic Thought Editor. Markets with asymmetric information. *Economic Thought Journal*, 1(6):93–108, 2001. (Nobel Prize winners on Economy for 2001).

[28] K.J. Arrow and G. Chichilnisky. *Markets, Information and Uncertainty: Essays in Economic Theory in Honor of Kenneth J. Arrow*. Cambridge books online. Cambridge University Press, 1999.

[29] Michael Spence. Job market signaling. *The quarterly journal of Economics*, 87(3):355–374, 1973.

[30] D.C. Rose. *The Moral Foundation of Economic Behavior*. Oxford University Press, USA, 2011.

[31] R.H. Frank. *Passions Within Reason: The Strategic Role of Emotions*. Norton, 1988.

[32] Benjamin Klein. The role of incomplete contracts in self-enforcing relationships. *Revue d'économie industrielle*, 92(1):67–80, 2000.

[33] Judith L Herman. *Trauma and recovery: The aftermath of violence–from domestic abuse to political terror*. Basic Books, 1997.

[34] Max Weber. Economy and Society. In H.H. Gerth and C. Wright Mills, editors, *Max Weber: Essays in Sociology*. Oxford University Press, New York, NY, 1946.

[35] Ludwig von Mises. *Bureaucracy*. Arlington House, New Rochelle, NY, 1969.

[36] R.E. Wagner. *Economic policy in a liberal democracy*. Shaftesbury papers. Edward Elgar, 1996.

[37] Hannah Arendt. *On violence*, volume 17. Mariner Books, 1970.

[38] Thomas James Ball. Last statement. In *The Keene Sentinel*. Keene Publishing Corp., Keene, NH, USA, 22 Jul 2011. (newspaper article).

[39] Steve Mann. *The Surveillance Scenarios*. Presented to at: "Identity, Privacy & Security by ReDesign", Monday 2012 October 22nd, 4pm to 5:30pm, Room 728, Bissell building, 140 St. George Street, http://wearcam.org/sousnarios.htm Archived as PDF and further time-stamped at: http://www.webcitation.org/6CbxqQU49, 2013.

[40] Steve Mann. Eye am a camera: Surveillance and sousveillance in the glassage. *Time Magazine*, 02 November 2012.

[41] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Programming / Security. Wiley, 1995.

[42] G.A. Stobbs. *Business Method Patents*. Aspen Pub, 2002.

[43] G.A. Stobbs. *Software Patents*. Aspen Pub, 2012.

[44] J. Erickson. Beware open source encryption. *Dr. Dobbs Journal*, Oct. 24th 2009.

[45] Free Software Foundation. *What is free software?* Free Software Foundation, 2012. http://www.gnu.org/philosophy/free-sw.html .

[46] John Perry Barlow. Decrypting the puzzle palace. In *Comm. of the ACM*, volume 35(7), pages 25–31. ACM Press, July 1992.

[47] John Gilmore. *Speech on Privacy, Technology, and the Open Society*. Presented at: "First Conference on Computers, Freedom and Privacy", 1991.