Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures

Lisa A. Shay and Gregory Conti
Cyber Research Center
United States Military Academy
West Point, NY 10996
{lisa.shay, gregory.conti}@usma.edu

Woodrow Hartzog
Cumberland School of Law
Samford University
Homewood, AL 35229
whartzog@samford.edu

Abstract—**The rapid decline in size and cost of networked sensors combined with increased incentives for use including monitoring physical fitness, improving public safety, increasing security, and adding convenience is causing the physical and online worlds to become heavily instrumented. Some welcome such developments, but others seek to retain privacy, often by focusing on countering the sensors themselves. Scholars have begun to consider surveillance countermeasures as a stand-alone area of research. However, a scholarly taxonomy useful for critical analysis and systematic countermeasure development is lacking. In this paper we provide such a taxonomy illustrated with example countermeasures that have been successfully employed.**

Keywords—panopticon, uberveillance, veillance, surveillance, privacy, countermeasures

I. INTRODUCTION

Surveillance and privacy are seemingly locked in a continual game of one-upmanship. In the security context, adversarial relationships exist where an attacker exploits a vulnerability and the defender responds with countermeasures to prevent future attack or exploitation. From there, the cycle continues, with new vulnerabilities and better exploits, against improved countermeasures. In the privacy context, many have feared the government as a highly empowered threat actor who would invasively and ubiquitously violate privacy, perhaps best personified by DARPA's Total Information Awareness initiative or Orwell's 1984 [1,2] However, commercial companies today offer enticing free products and services in return for user information, examples include search, social networking, email, and collaborative word processing, among myriad other offerings, leading to instrumentation, data collection, and retention on an unprecedented scale. End users, small business, and local governments themselves are often complicit by supporting, enabling, and conducting such activities. Whether a dystopia exists in our future remains to be seen, although we argue panopticon-like environments exist in today's authoritarian regimes and increasingly surveillance is becoming embedded in the fabric of Western society to thwart terrorism, increase business efficiency, monitor physical fitness, track driving behavior, provide free web search, and many other compelling incentives.

Not all are willingly subject to pervasive surveillance. Many people employ countermeasures to frustrate collection practices for many reasons, including to lead a more private life, perform illicit activities, or protect those with whom they interact. Such countermeasures are the subject of this paper. In order to ground the work, we first define privacy and countermeasures. There are many definitions, but for our purposes the definition from Merriam-Webster is suitable [3]. Privacy is "the quality or state of being apart from company or observation" or "freedom from unauthorized intrusion." For the definition of countermeasures we draw upon U.S. military doctrine and define countermeasures as mechanisms that "deter, deny, disrupt, deceive, dissuade, degrade, destroy and defeat" surveillance systems and privacy degrading mechanisms and regimes [4]. More broadly, we examine "the employment of devices and/or techniques, [that] has as its objective the impairment of the operational effectiveness," [5] in this case the operational effectiveness of networked surveillance systems.

Our primary contribution is a detailed and extensible taxonomy that enables a systematic pursuit of effective surveillance countermeasures suited for the particular social, political, economic, and technological context. While work has been done on the study of individual instances of surveillance countermeasures and to some extent, slightly broader analyses of families of countermeasures, an overarching countermeasure taxonomy has not yet been presented. A thorough taxonomy is useful to privacy advocates, security practitioners, policy makers, and privacy researchers as well as groups and individuals interested in increasing their personal and collective privacy.

We focus on surveillance countermeasures and privacy in the physical world, but because such instrumentation cannot be dealt with in isolation from the Internet, we also include limited coverage of online countermeasures. Our goal is to be comprehensive, but not exhaustive. New countermeasures are developed on a regular basis and others are so ancient that that evolution has imbued them into the genetic structure of animals, such as the color changing ability of chameleons or the camouflaged pelts of leopards. It is important to note that we do not advocate usage of any given countermeasure, as such usage may be morally wrong or illegal in a given context.

It is difficult to categorically validate any taxonomy, due to unknown potential extensions, but we conducted significant due diligence by gathering countermeasure samples from major popular and technology news sources as well as major privacy watchdog groups including the Electronic Frontier Foundation and the Electronic Privacy Information Center for the past 37 months. We have carefully reviewed these approximately 420 news stories, white papers, and scholarly articles, to inform and

build out the taxonomy. Due to space constraints, we did not include every example, but carefully selected representative examples and provided extensive citations. In addition, we presented work-in-progress talks to two major hacker conferences, DEFCON and HOPE, to help validate our approach, methodology, and findings [6,7].

This paper is organized as follows. Section II places our work in the field of related research. Section III presents a model of networked sensor systems. Section IV presents our taxonomy and Section V provides our conclusions and promising directions for future work.

II. Related Work

Leading electronic privacy-rights groups such as the Electronic Frontier Foundation and Electronic Privacy Information Center have conducted significant work easily characterized as privacy countermeasures, most notably privacy countermeasures based on policy, but they have not developed taxonomies. Similarly, academic conferences such as the Privacy Enhancing Technologies Symposium (PETS) and the Workshop on Privacy in the Electronic Society (WPES) have published numerous technical articles on privacy countermeasures, but again not an overarching taxonomy. The Workshop on the Economics of Information Security (WEIS), provided significant insight into individual and collective incentives driving human actors and surveillance subjects [8]. These privacy groups and academic conferences, across their complete range of activities and bodies of work, provide extensive examples of countermeasures and, in many ways, emergent countermeasure taxonomies. We leverage this fact to inform our work.

Lawrence Lessig provides detailed analysis on "responses," effectively countermeasures, to privacy risks via four modalities: law, norms, markets, and architecture/code [9]. We carefully considered each modality as a potential root level entry in our taxonomy. Daniel Solove provided a thoughtful privacy taxonomy to help identify and understand privacy violations and included information collection, information processing, information dissemination, and invasion high-level categories [10]. While Solove did not focus on countermeasures, his categorization of privacy threats can be studied category-by-category to help guide potential countermeasure analysis and development.

Clarke suggests eight principles for counterveillance (countering surveillance) including independent evaluation of technology, a moratorium on technology deployments, open information flows (transparency), proper justification, public consultation and participation, cost/benefit evaluation, rollback of anti-freedom provisions and laws, and incorporation of design principles that facilitate balance, anonymity, multiple identity, and independent control [11]. We have carefully integrated these principles into our taxonomy.

Military doctrine and tactics also provide useful insights into privacy countermeasures including two contexts: Countering Improvised Explosive Devices (IEDs) and battlefield deception. Shoop's countering IED tenets included mitigating effects of the IED (e.g. via an armored vehicle), defeating the device (e.g. a jammer that blocks IED command signals), targeting the emplacer, targeting funding networks, and disrupting supply chains [12]. This multi-layered approach illustrates the power of targeting the *system* not just an isolated component, however this taxonomy makes assumptions about the illegality of the activity (i.e. IED usage). In the context of privacy threatening technologies and regimes the activities may or may not be illegal. Military organizations have employed deceptive countermeasures, such as bluffs, camouflage, false radio traffic, and mocked-up equipment for centuries. A study of these battlefield deception techniques is useful to the study of privacy countermeasures. Latimer provides an excellent survey [13].

Schneier's taxonomy of social networking data which includes service data, disclosed data, entrusted data, incidental data, behavioral data, and derived data categories, does not suggest countermeasures, but is illustrative of the overt and covert ways sensitive data is generated [14]. Conti provided similar analysis in *Googling Security*, but in the context of web search, email, mapping, and third-party tracking on the web. He suggests web-based information disclosure countermeasures in three major categories: user-centric measures, technical protection, and policy protection [15]. We also commend study of Reidenberg and Cranor's work on the Platform for Privacy Preferences (P3P). P3P is a World Wide Web Consortium (W3C) specification to communicate machine readable privacy preferences. Given the complexity, and often ubiquitous, nature of automated surveillance, countermeasures that can operate at machine speed are particularly of interest for the surveillance countermeasure researcher [16].

III. Model

There are many components of a networked surveillance system, each of which may be subject to countermeasures, and an understanding of these components is essential to the development of our taxonomy. In previous work, we developed a framework for networked surveillance systems, a simplified version is shown in Figure 1 [17]. The framework consists of classes (the colored rectangles) with attributes that describe how the class performs in the surveillance system. These classes are grouped into sets that include people (actors and subjects) and components (the hardware and software that forms the networked surveillance system). In its general form a networked surveillances system utilizes sensors (both active and passive) that measure energy in the environment. For example, an acoustic sensor measures the pressure of sound waves and the charge coupled device (CCD) in a camera measures visible light. The camera may rely upon ambient light (passive sensor) or use a flash (active sensor) to generate improved results. In a digital system the measured energy is quantized and stored, and may undergo local processing and local access by human or machine. The resultant information is then transmitted across a network where the data generated by many sensors is aggregated and stored in centralized systems. The information then undergoes additional processing and data mining, and is consumed by more human and machine users. The process iteratively continues as the information is further stored, processed, refined and shared with additional users and systems. Such systems are rarely foolproof or leakproof, as each class in the model has

vulnerabilities, including human actors and surveillance subjects. For instance, information may be corrupted, leaked, destroyed, or shared under a variety of circumstances including malfeasance, accident, or legal pressure. Our earlier work acknowledged these vulnerabilities without elaborating on them. The taxonomy that follows examines the categories and classes in our model, discusses their vulnerabilities, and then describes corresponding countermeasures that exploit those vulnerabilities. Given that some vulnerabilities are common to multiple classes, there are some countermeasures that are listed in more than one table in the taxonomy.

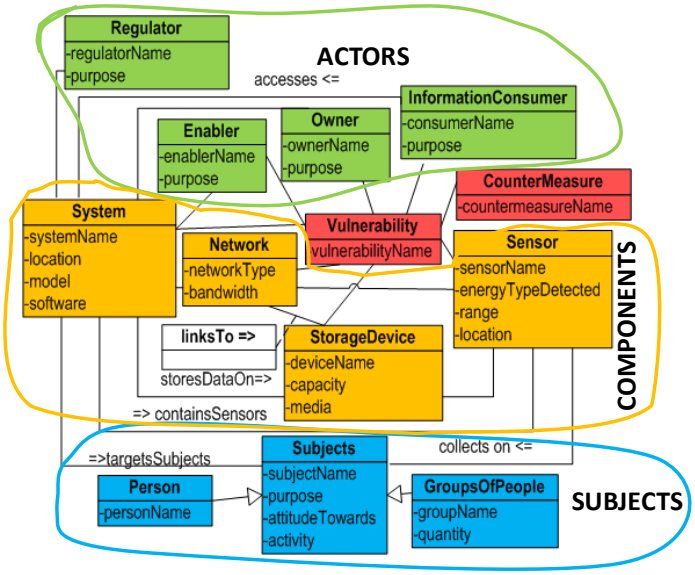

Figure 1. Networked surveillance system framework, consisting of human actors, system components, and surveillance subejcts [14]. Each entity possesses vulnerabilities from which countermeasures may be derived.

IV. TAXONOMY

Although sensors are the most obvious and visible aspect of a sensor system, we begin our analysis with the actors, since the people who design, build, own and operate networked surveillance systems have the most control over their function and use. Effectively countering the actors produces significant and lasting impacts on the surveillance system.

A. Actors

Our taxonomy consists of two groups of people: actors and subjects. The actors are responsible for creating, deploying, and using networked sensor systems. Subjects are surveilled by those systems. We distinguish these groups because the classes of actors have very different motivations and purposes than the subjects. In the interplay of measures, countermeasures, and counter-countermeasure, the actors and subjects usually form the opposing sides. As noted in [17], owners, enablers, and information consumers often share similar purposes and so there are countermeasures common to all three of those classes. Those form the "common" category in Table I.

1) Owners

Owners have many incentives for creating these networked sensor systems: they want to increase the safety and security of their home or office building, they want to use energy or other resources more efficiently, or derive some other benefit from the data collected such as improving personal or employee health or enjoy greater convenience. Businesses and law enforcement officials are common kinds of owners. Eventually, some owners may wish to sell the information collected. This last incentive may not have been the original reason for setting up the system, but once the system is in place and collecting useful and valuable data, there is a temptation to use this data for financial gain, particularly in business contexts. To deter owners from employing overly-invasive sensor systems, or encourage them to remove existing ones, we suggest surveillance countermeasures that target incentives, see Table I.

2) Enablers

Enablers are the people and organizations that design, build, sell, or rent networked sensor systems or their components. For example, those that design, build and install CCTV cameras are enablers. While some enablers might be inspired by patriotism or a desire to increase public safety or wellness, their main incentive is often profit, which can be threatened in many ways, as shown in Table I.

3) Information Consumers

Information Consumers retrieve and utilize the collected data, often aggregated from multiple sensor systems. They have many incentives, such as financial gain, increasing security, monitoring physical fitness and health, improving public safety, adding convenience, even voyeurism. As an example, building security personnel monitor fire and intrusion detection systems to improve building security and the safety of its occupants. Individuals may use a variety of sensors including ones to measure heart rate, caloric intake, blood sugar, and body weight to improve their health or physical fitness. Public safety personnel employ many sensors and sensor systems including radar detectors, red-light cameras, surveillance cameras, drones, and robots to improve public safety. Consumers employ home security systems; home energy monitoring systems, smart phones with cameras, microphones, accelerometers and GPS receivers; E-ZPass toll collection systems; credit cards and vendor loyalty cards; automotive sensor systems like OnStar® and others to improve their security, save money, or add convenience to their lives.

4) Regulators

The regulator class enables, limits, or restricts the capabilities of networked sensor systems in some way. Regulators are usually part of government, but could also be independent organizations such as trade groups or professional societies like the IEEE. In the case of government regulatory agencies such as the FCC or FAA, regulation may be their primary purpose. For trade groups and professional societies, regulatory activity may be just one of many activities. Trade groups and professional societies may regulate directly by developing standards, or indirectly by lobbying government to change a law or regulation. There are two primary types of regulator surveillance countermeasures: actions regulators can take to reduce the damage from sensor networks and actions the public can take to induce regulatory bodies to enact protections. These are shown in Table II.

B. Subjects

Subjects, individually and collectively, are the targets of sensor systems. To reduce the invasion of their privacy, subjects can take actions to simply protect themselves, such as wearing a disguise, opting out of data sharing, or deciding not to use certain technologies. Some of these actions will make life less convenient, so subjects balance their privacy interest with whatever benefit they derive from surveilled activity, if any. Subjects can also take actions that protect others as well as themselves, such as advocating for greater regulation or the removal of a red-light camera system in their town. Subject countermeasures are shown in Table III.

C. Components

We identify four classes of components in a networked sensor system, shown in Figure 1: system, network, storage, and sensor. Each class has attributes and many of the attributes have vulnerabilities against which a subject can perform a countermeasure. Alternatively, the owners, enablers and information consumers are interested in fixing the vulnerabilities and countering the countermeasures in a feedback control system, or a sort of surveillance "arms race." We categorize component countermeasures in Table IV. Note that each day a person can encounter dozens of sensors, so many that we hardly pay any attention to them. In [17] we presented a case study of "Hal," an ordinary citizen going about a very ordinary life; going to the gym, going to work, shopping at a supermarket; who was monitored by at least 20 sensors in an 18-hour period.

V. Conclusions and Future Work

When considered as a whole, the range of potential surveillance countermeasures is dramatic and growing. We believe the taxonomy we present is useful in its current form, but recommend that it be extended as new techniques and strategies emerge. As the development of new sensors and surveillance systems begs the use of countermeasures by the surveilled, the use of countermeasures also invites the development and use of counter-countermeasures. Examples of counter-countermeasures include the use of lobbyists to influence policy makers or a police officer pointing a gun to discourage a videographer filming a police raid, among myriad others [18]. This vicious cycle results in a continued game of one upmanship, or a contest of resources and resolve to determine a victor. For future work we recommend the development of a comprehensive taxonomy of counter-countermeasures to complement this paper. Similarly, our work focused on countermeasures in the physical world, we believe a detailed survey of online countermeasures, particularly in the context of the World Wide Web, would be a valuable research contribution. Future work in system design is also promising. System designers are not immune to the security and privacy implications of their designs. By providing classical security protections, such as confidentiality, integrity, and availability good designers help ensure secure operation and prevent information leakage, data spills, or eavesdropping by unauthorized parties. Even better, from the perspective of the surveilled, are systems that actively include privacy by design.

This taxonomy categorizes countermeasures, but one should not infer that countermeasure are always employed independently. To achieve the greatest effect countermeasures are often woven together into campaigns of mutually supporting activities. We see such campaigns in military battlefield deception operations, intelligence community counter-surveillance activities, actions of governmental and industry chief privacy officers, and long-term efforts of privacy advocacy groups such as the EFF, EPIC, and the ACLU. In complex campaigns, actors seek to holistically identify surveillance practices and deny, degrade, defeat, or destroy varying parts of the surveillance system for maximum effect through the use of many countermeasures. A comprehensive campaign may seek to undermine incentives of both aggressors and subjects, identify and share location of sensors, seek to create false positives, cause physical destruction of system components, prevent the deployment of sensors and systems, anticipate and counter future aggressor actions, train subjects in counter-surveillance techniques, and exploit weaknesses in the technology and human networks underpinning the surveillance activity, among numerous other strategies.

A taxonomy of countermeasures is useful for critical analysis, but it is only a starting point. For future work, we suggest seeking quantitative means, including suitable equations, metrics, and models, to analyze the efficacy, effectiveness, and risk associated with surveillance countermeasures. Such calculations could take into account factors such as security personnel response time, effort, cost, power requirements, legal authority, system vulnerability, attack surface, actor and subject incentives, data retention policies, data collection policies, and processing strengths and weaknesses. Similarly, models could include insight into how systems are employed and what countermeasures could be used to degrade or defeat various capabilities of the system. Importantly, models could help identify gaps for which no countermeasures exist and drive future research and development.

Targeted surveillance countermeasures (e.g. countermeasures that seek to degrade or defeat specific sensor, system, or processing technologies) are ripe for future exploration. For example, every sensor has limitations that result in some degree of error, how can these weaknesses be exploited to develop more successful countermeasures? In addition, many surveillance systems seek to detect subjects, and if possible, uniquely identify individuals. Is it possible to categorize countermeasures whether they defeat identification algorithms, (e.g. facial recognition) or defeat the more general, and likely more difficult detection (e.g. facial detection) algorithms? And every countermeasure has the potential to itself be countered, as in the model of John Boyd's "Observe-Orient-Decide-Act" (OODA) loop [19]. The legality of any specific countermeasure (and its corresponding counter-countermeasure) is open to question, especially if one is countering the "system," "network," or "storage device" components of our model by " hacking back" [20].

Finally, we suggest further exploration of the societal implications of widespread surveillance, even in contexts where the subject is complicit or the government is well intentioned. Sensors are becoming increasingly prevalent and

the future portends sensing of human activities on a global scale of unprecedented proportion. Surveillance networks and the use of countermeasures modify behavior, both individual and in aggregate. When is this good and when is this bad? As a society, perhaps the most important tool is regulators seeking appropriately balanced solutions and "honest" consulting, and not coercion, deception or attempts at desensitization, with the observed regarding surveillance programs. As Lessig famously said, "code is law" [21]. If average citizens, not just criminal actors operating outside the law, feel the need to develop and employ countermeasures perhaps societies should reconsider the use of such privacy invasive technologies.

TABLE I OWNER, ENABLER, AND INFORMATION CONSUMER COUNTERMEASURES

Class of Surveiller	Surveillance Countermeasure	Examples
Common	***Inconvenience***	Administrative burdens, such as additional paperwork, can be tantamount to prohibition
	Reputation Tarnishment	Call out bad behavior; publish embarrassing news stories [22-26]
	Financial Loss	Loss of customers or drop in stock price due to privacy gaff [27]; lawsuits [28]; payment of compensations [29]; pay for privacy business models [30]
	Harassment	Reverse robocalling government leaders [31]
	Legal Restriction	Enact federal, state, and local legislation to prohibit or constrain privacy damaging behavior; modify or strike down poorly written law [33, 33]; threaten legal action [34]; investigate suspect practices [35]
	Praise	Praise positive behavior to reinforce success [36]
	Regulation	Policy that prohibits undesired behavior [37]
	Physical Retaliation	Personal threats (or worse) against actors enablers, system owners, regulators, or information consumers [38]
Enablers	***Regulatory Compliance***	Administrative burdens such as compliance testing or licensing requirements for designers or installers can make the cost of development, production, deployment, and use prohibitive.
	Legal monopolies	Protective patents to prevent adoption of privacy threatening technologies [39].
Info. Cons.	***Data Access***	Prevent or disrupt access to data, possibly by disrupting the sensor network itself.

TABLE II REGULATOR COUNTERMEASURES

	Regulator Countermeasure	Examples
	Demand Accountability	Google settles with FTC over tracking cookies, pays $22.5M fine [49] Congress questions Google about Glass [40]
	Enact privacy and data protection laws	European Union plan to enact data protection law [41]
	End use of privacy invasive systems	Los Angeles considers ending use of traffic light cameras [42]
	Increase Procedural Burdens	Require warrant for access to data not informal law enforcement request; limit warrantless laptop searches at borders [43]
	Investigate	FTC orders information from information brokers [44]; TSA commissions independent study of X-Ray Body Scanners [45]; Congressional hearings on TSA scanners [46]; require validation and justification for usage of privacy-threatening systems
	Substantive Legal	New York State law makes gun ownerships records private (albeit as an opt-in process); regulations that

	Privacy Protections	limit commercial imagery satellite resolution [47]
	Regulate Use of Surveillance Technologies	European Commission adopts rules regulating use of security scanners at European airports [48].
Encourage regulators	***Engage Decision Makers***	Target political support; vote for politicians supportive of privacy; participating in town hall events [50]; visiting decision makers in their workplace; contribute to public outcry over privacy-invasive actions and threats [51]; raise safety concerns about sensor technology [52]
	Go to court	Sue companies with suspect privacy practices [53]; German state of Hamburg considers fining Facebook over facial recognition feature [54]; U.S. Supreme Court rules on use of GPS devices [55]

TABLE III SUBJECT COUNTERMEASURES

Class	Subject Countermeasure	Examples
Indirect Countermeasures to Protect Oneself and Others	**Activism**	Take personal [56, 57] or collective action to lobby against bad behavior, pending laws [58-60]; lobby officials for better privacy practices; participate in public debate; Camover game which challenges participants to destroy surveillance cameras [61]; civil disobedience (e.g. Tahrir Square); formation of political party (e.g. Pirate Party), formation of own country (e.g. Principality of Sealand); hactivism (e.g. Anonymous);
	Conduct and Publish Research	Suggest viable alternatives such as anonymized airport scanner views [62]; point out security flaws in surveillance systems[63]; develop systems that allow opting out of sensing [64]; Solove's "I've Got Nothing to Hide" [65]; produce research that is admissible in court; EFF's Panopticlick project [66]
	Create and share influential media	Create viral videos; write science fiction on potential privacy risks (Doctorow's Little Brother); create movies warning of privacy risks (e.g. Minority Report, Gattaca); write non-fiction studies of privacy abuses such as East Germany and McCarthy-era America; culture jamming graffiti; Google's anti-SOPA graphics [67]
	Create competing technologies, organizations or companies that respect privacy	Creation of an open source search engine[68]; private social networks, darknets, or ISPs [69-71]; offer reward for countermeasure development [72]; provide awards for individuals and organizations promoting privacy [73, 74]; host contests for developing privacy enhancing technologies[75]
	Contribute	Run Tor exit node
	Educate	Educate populace on privacy issues and solutions via popular press[76-78], college courses [79], privacy groups [80,81]; publish human-readable translations of legal documents [82]; seek self-education on privacy matters; give media interviews, learn how to engage the media [83].
	Form Collectives and Alliances	Stop Online Piracy Act (SOPA) Blackout Day which included Wikipedia, Google, Mozilla Foundation, and BoingBoing among numerous others; support for privacy groups such as the EFF and EPIC; join a professional society with policy outreach efforts (e.g. IEEE and ACM)
	Vote	Vote for officials that support privacy; avoid doing business with companies and governments that do not respect privacy
Direct Countermeasures to Protect Oneself	***Avoid Generating Data***	Live an off the grid lifestyle; use traditional postal service versus electronic mail; use paper money instead of electronic cash; avoid Facebook "liking" of web pages; run ad-blocking software; use Firefox Private Browsing mode that does not save visited pages, form and search bar entries, download list entries, cookies, and cached web content [84]
	Maintain Multiple Personas	Create throw-away online identities; create identities which disclose only sufficient information for a given transaction
	Employ privacy-enhancing technologies	DoNotTrackMe add on for Firefox [85]; application layer encryption such as PGP; Off-the-Record (OTR) encryption software for instant messaging; high-grade encryption smart phone apps [86]; install ad blockers [87, 88]; disable referer data from web browsers; use reputation management software [89]
	Maintain Security Awareness	Assume surveillance[90]; assume data and hardware will be confiscated or stolen [91, 92]; be observant for government, commercial, private, and criminal sensors, such as an illicit card swipe scanner [93]

	Monitor Application Behavior	Watch for "canaries" (particular pieces of sensitive information) being transferred [94], monitor smart apps for data leakage [95]
	Obfuscation	Corrupt the integrity of personal disclosures by lying or otherwise obfuscating personal information with false, ambiguous, misleading or irrelevant information [96]
	Take Personal Responsibility	Apply common sense; read terms of service and other agreements; don't disclose information without due cause particularly when using social networks [97]; report malfeasance to regulators and law enforcement
	Use more secure hardware and software	Russia creates secure "Almost Android" tablet [98]; web camera with opaque shield that flips down over lens; hardware disconnect for microphone; Tor Browser Bundle [99]; notify user when encrypted channel fails; carry completely reimaged computer in high threat environments; use privacy filter or privacy glasses for viewing monitor to prevent shoulder surfing; employ tamper detection techniques that indicate if computer case was opened

TABLE IV COMPONENT COUNTERMEASURES

Class	Countermeasure	Example
Storage	***Encrypt***	Mandate employment of full disk encryption[100, 101]; salt and hash password databases
	Anonymize	Delete data fields; perform data aggregation; do not link data with real world identities; do not provide identifying information in email
	Avoid Cloud Services	Privacy expert Caspar Bowden warned Europeans not to use cloud services hosted in U.S. [102]
	Corrupt	Overwrite random fields in database
	Destroy data or device	Policies that routinely and effectively destroy unnecessary information; delete data using forensically sound techniques; degaussers; shredders
	Limit Data Sharing	Policies that limit sharing of data within a company and with third-parties; policies that protect data during bankruptcy or sale of company
	Prevent User Tagging	Disable third-party cookies in web browsers; enact Do Not Track policy [103, 104]
	Prevent Data Collection	Organizational policy that prohibits data collection; system architecture that does not collect data; avoid collecting sensitive data such as personally identifiable information (PII); if you cannot properly secure data do not collect it; collect only information necessary for system function [105]
	Resource Consumption	Overflow storage of logging server
	Transparency	Clearly explain to users what information is being collected as well as other policies; policies that mandate disclosure of data spills
Network	***Anonymity Network and Proxies***	Tor; I2P
	Air Gapped Networks	Avoid connecting sensitive data or systems directly to the Internet
	Architecture	Place sensitive systems or servers far from public facing DMZ
	Use Non-attributable Network Access	Use public wireless hotspots, unsecured or poorly secured wireless access points, disposable phones, pay phones; boot from CD/DVD/USB operating system distributions
	Encryption	Employ HTTPS to reduce possibility of eavesdropping; develop browser add-ons to increase usability of encryption techniques [106]; do not write own "custom" cryptographic code; use VPNs; use SSH
	Jamming	Wireless jammers [107]
	Sneaker Net	Employ human or animal couriers; communicate via paper and pen
	Spoof Network Identity	Spoof IP or MAC address [108]

System	***Analyze System***	Acquire similar, or exact, components, disassemble, read specification sheets, understand range, power consumption, processing ability, sampling rate, response time, sensitivity, maintenance condition, limitations, and vulnerabilities [109]
	Attack the System	Probe for weakest link; target key nodes [110]
	Allow user choice	Create opt-in (vs. opt-out) choices for users
	Notice	Notify users when system is in operation [111]
	Overcome Processing	Take every case to trial and overwhelm court system [112]
	Privacy Policies	Create human-readable (vs. lawyer-readable) privacy policies;
	Securely lock down systems	Guides for securing systems [113]; employ multi-factor authentication; securely configure and routinely patch systems
Sensor	***Avoid***	Operate when sensor is non-functional, or not in operation; move out of sensor range
	Camouflage	Defeat detection or identification by either human or machine intelligence analyzing sensor data [114], CV Dazzle make-up and hairstyle techniques to defeat detection [115, 116]
	Challenge calibration	Confirm that the sensor been properly and recently calibrated; confirm that the calibration certifying authority is accredited to perform such calibrations
	Degrade signal received by sensor	Employ shield to block emissions [117]; employ obscurant [118]; radar absorbing paint, velcro tab that covers Infrared reflector on U.S. military combat uniforms, Near-Infrared compliant uniforms that reduce IR emanations; Metamaterials that could form an “invisibility cloak” [119] use of highly insulated fire proximity suit to reduce thermal emissions; RFID blocking wallets, Wi-Fi shielding wallpaper; placing cardboard box over traffic camera; deliberate introduction of disinformation
	Detect	Radar detectors for automobiles; Shodan search for online devices
	Disable	Physical destruction, disrupt power source; HERF weaponry; placing black tape over optical sensor, using a microphone plug in laptop audio in to disable microphone at hardware level
	Disclose location of sensor	Identify and share locations of speedtraps [120]; New York City Surveillance Camera Project; governmental posting of traffic camera locations
	Exceed capabilities	Operate outside range, sensitivity, or resolution of sensor; operate in mode that cannot be detected by a given type of sensor; understand range and coverage of sensor; bypass field of view of sensor; moving very slowly to fall below triggering threshold of motion sensor; employ air-gap or stand-off distance from emanations to potential sensor locations
	Jam	Subject-owned flash that triggers in response to photographic flash [121,122]; directing laser into optical sensor
	Monitor	Cameras that watch other cameras [123], note that this story illustrates the use of additional cameras to monitor attacks against law enforcement speed sensors, we suggest that similarly using sensors to monitor sensors as a viable privacy countermeasure.
	Planned Obsolescence	Sensors that become inoperable after a given period.[124]
	Provide false information	Create fake identities or personas [125]; inflatable tanks, false heat generators to fool thermal sensors

VI. REFERENCES

[1] Jeffrey Rosen. "Total Information Awareness." New York Times, 15 December 2002.

[2] George Orwell. *Nineteen Eighty-Four*. Secker and Warburg, 1949.

[3] "privacy." Merriam-Webster Dictionary Online.

[4] Kamal Jabbour. "50 Cyber Questions Every Airman Can Answer." Air Force Research Lab, 2008.

[5] Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*" Joint Publication 1-02, 8 November 2010.

[6] Greg Conti. "Our Instrumented Lives: Sensors, Sensors, Everywhere." DEFCON 18, July 2010.

[7] Lisa Shay and Greg Conti. "Countermeasures: Proactive Self-Defense Against Ubiquitous Surveillance." Hope Number 9, New York City, 13-15 July 2012.

[8] "The Twelfth Workshop on the Economics of Information Security (WEIS 2013)." Georgetown University, 11-12 June 2013. See http://weis2013.econinfosec.org/, last accessed 26 January 2013.

[9] Lawrence Lessig. CODE Version 2.0. Basic Books, 2006.

[10] Daniel Solove. "A Taxonomy of Privacy." University of Pennsylvania Law Review, Vol. 154, No. 3, pp. 477-560.

[11] Roger Clarke. "What is Uberveillance (And What Should Be Done About It?)." *IEEE Technology and Society Magazine*, Summer 2010, Vol. 29, No. 2, pp. 17-23.

[12] Glenn Zorpette. "Countering IEDS," *Spectrum, IEEE* , vol.45, no.9, pp.26-35, September 2008.

[13] Jon Latimer. "Deception in War." Overlook, 2003.

[14] Bruce Schneier. "A Revised Taxonomy of Social Networking Data." Schneier on Security, 10 August 2010.

[15] Greg Conti. Googling Security. Addison-Wesley, 2009.

[16] Joel Reidenberg and Lorrie Cranor. "Can User Agents Accurately Represent Privacy Policies?" Working Papers Series, SSRN = 328860

[17] Lisa A. Shay, Gregory Conti, Dominic Larkin, John Nelson, "A Framework for Analysis of Quotidian Exposure in an Instrumented World." International Carnahan Conference on Security and Technology, 15-18 October 2012, Boston, MA.

[18] Glyn Moody. "EU Data Protection: Proposed Amendments Written by US Lobbyists." *Computerworld UK*, 11 February 2013.

[19] William S. Lind, *Maneuver Warfare Handbook*, London: Westview Press, 1985.

[20] Jayaswal, V.; Yurcik, W.; Doss, D., "Internet hack back: counter attacks as self-defense or vigilantism?," *International Symposium on Technology and Society, 2002. (ISTAS'02)*, pp.380-386, 2002.

[21] Lawrence Lessig. "Code is Law: On Liberty in Cyberspace." Harvard Magazine, January-February 2000.

[22] Elinor Mills. "Google Balances Privacy, Reach." CNET News, 14 July 2005.

[23] Mat Honan. "How Apple and Amazon Security Flaws Led to My Epic Hacking." Wired Gadget Lab Blog, 6 August 2012.

[24] Scott Calvert. "City Issued Speed Camera Ticket to Motionless Car." Baltimore Sun, 12 December 2012.

[25] "Andrea Fornella Abbott Arrested For Yelling At TSA Over Daughter's Patdown." Huffington Post, 13 July 2011.

[26] Spencer Ackerman. "Pentagon Swears It Won't Sell Killer Drones to Afghanistan, Just Spy Ones." Wired Danger Room Blog, 15 January 2013.

[27] "Facebook Privacy." Electronic Privacy Information Center. http://epic.org/privacy/facebook/, last accessed 26 February 2013.

[28] Loek Essers. "Facebook Sued Over App Center Data Sharing In Germany." TechWorld, 7 December 2012.

[29] Erica Ogg. "Sony to Restore PSN Services, Compensate Customers." CNET News, 30 April 2011.

[30] Janice Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." Journal of Information Systems Research, Vol. 22, No. 2, June 2011, pp. 254-268.

[31] Sean Gallagher. "'Reverse Robocall' Campaign Lets Citizens Phone-Blast SOPA Supporters." *Ars Technica*, 27 December 2011.

[32] Megan Geuss. "California State Legislature Approves Location Privacy Act." Ars Technica, 22 August 2012.

[33] Loek Essers. "German Privacy Regulator Orders Facebook to End Its Real Name Policy." ITworld, 17 December 2012.

[34] Anne Saita. "California Attorney General Puts Mobile App Developers on Notice." Threat Post Blog, 30 October 2012.

[35] Preston Gralla. "Privacy Group Asks FTC to Investigate Google." *PC World*, 18 May 2009.

[36] Lucian Constantin. "Facebook to Roll Out HTTPS by Default to All Users." Computer World, 20 November 2012.

[37] Natasha Singer. "New Online Privacy Rules for Children." New York Times, 19 December 2012.

[38] Regina Wang. "Newspaper Hires Armed Security Guards After Backlash Over Gun-Owner Map." *Time Newsfeed*, 2 January 2013.

[39] Philip Zimmermann. "The Unveiling of My Next Big Project: ZPhone." Defcon 13, 2005.

[40] "US politicians quiz Google on Glass privacy," BBC News, 17 May 2013. See http://www.bbc.co.uk/news/technology-22567061, last accessed 22 May 2013.

[41] Anna Leach. "Upcoming EU Data Law will Make Europe Tricky for Facebook." *The Register*, 8 November 2011.

[42] Joel Rubin. "L.A. Traffic Cameras May Get the Red Light." Los Angeles Times, 8 June 2011.

[43] Stephanie Condon. "Bill Would Limit Homeland Security Laptop Searches." CNET News, 30 September 2008.

[44] "FTC to Study Data Broker Industry's Collection and Use of Consumer Data. Federal Trade Commission, 18 December 2012.

[45] Michael Grabell. "TSA to Commission Independent Study of X-Ray Body Scanners." ProPublica, 18 December 2012.

[46] "Transportation Security Subcommittee to Hold Hearing on TSA Body Scanners." U.S. Committee on Homeland Security, 14 November 2012.

[47] "World's Highest-Resolution Commercial Satellite." *Science Daily*, 27 May 2009.

[48] "Aviation Security: Commission Adopts New Rules on the Use of Security Scanners at European Airports." European Commission Press Release, 14 November 2011.

[49] Dennis Fisher. "Google Settles With FTC Over Tracking Cookies, Pays $22.5M Fine." Threat Post Blog, 9 August 2012.

[50] "TSA Oversight Part III: Effective Security or Security Theater?" U.S. Committee On Oversight and Government Reform, 26 March 2012.

[51] Bill Toland. "Some Find Pennsylvania's Tax Amnesty Ads Too Scary." *Pittsburgh Post-Gazette*, 29 March 2012.

[52] Marty Jerome. "New Study Says Traffic-Light Cameras Cause Accidents." *Wired*, 12 March 2008.

[53] "Apple Users Launch Privacy Campaign Against Google." BBC, 28 January 2013.

[54] Emil Protalinski. "German State to Sue Facebook over Facial Recognition Feature." ZDNet, 10 November 2011.

[55] Liptak, Adam, "Court Casts a Wary Eye on Tracking by GPS," New York Times, 8 November 2011.

[56] Cameron Scott. "Berners-Lee: Demand Your Data from Internet Companies." IT World, 19 April 2012.

[57] David Kravets. "School Kicks Out Sophomore in RFID Student-ID Flap." Wired Threat Level Blog, 18 January 2013.

[58] Max Smolaks. "Wikipedia's Jimmy Wales is Ready to Fight Snooper's Charter." Tech Week Europe, 6 September 2012.

[59] "Newcastle University Students Protest Biometric Scanner Move." The Northern Echo, 14 December 2012.

[60] Shane Richmond. "Instagram: We Won't Sell Your Photos." The Telegraph, 19 December 2012.

[61] Kim Zetter. "German Activists Punch Out Big Brothers Eyes." Wired Danger Room Blog, 31 January 2013.

[62] Jack Nicas. "TSA to Halt Revealing Body Scans at Airports." Wall Street Journal, 18 January 2013.

[63] Tom Cross. "Exploiting Lawful Intercept to Wiretap the Internet." Black Hat DC 2010.

[64] Victor Tiscareno, Kevin Jonhson, and Cindy Lawrence. "Systems and Methods for Receiving Infrared Data with a Camera Designed to Detect Images Based on Visible Light." U.S. Patent Application 20110128384, 2 June 2011.

[65] Daniel Solove. "I've Got Nothing to Hide and Other Misunderstandings of Privacy." San Diego Law Review, Vol. 44, No. 44, 2007, pp. 745-772.

[66] Peter Eckersley. "How Unique is Your Browser?" Privacy Enhancing Technologies Symposium, 2010.

[67] "Take Action." Google. https://www.google.com/takeaction/, last accessed 1 February 2013.

[68] Klint Finley. "Your Own Private Google: The Quest for an Open Source Search Engine." Wired Enterprise Blog, 7 December 2012.

[69] Rachel Metz. "A Social Network Built for Two." *MIT Technology Review*, 30 March 2012.

[70] Emil Protalinski. "Banned from Google+, Anonymous Creates Anonplus." Techspot, 16 July 2011.

[71] James Hutchinson. "No-frills NBN Provider Aims for the Tech Savvy: Engineers From Members-only Utility." IT News, 20 July 2012.

[72] Amy Gahran. "Hate Illegal Robocalls? FTC Offers $50,000 to Help Stop Them." CNN Tech, 19 October 2012.

[73] "EFF Pioneer Awards 2012." Electronic Frontier Foundation. https://www.eff.org/awards/pioneer, last accessed 21 January 2013.

[74] "EPIC Gives 2012 Privacy Champion Awards to Canadian Privacy Commissioner, Privacy Technologist." Electronic Privacy Information Center, 26 January 2012. http://epic.org/2012/01/epic-gives-2012-privacy-champi.html, last accessed 21 January 2013.

[75] "The Wall Street Journal Data Transparency Weekend." The Wall Street Journal, 13-15 April 2012. http://datatransparency.wsj.com/, last accessed 21 January 2012.

[76] "Facebook & Your Privacy." Consumer Reports, June 2012.

[77] "What They Know." Wall Street Journal, 2010-Present. http://online.wsj.com/public/page/what-they-know-digital-privacy.html, last accessed 26 February 2013.

[78] Natasha Singer. "A Trail of Clicks, Culminating in Conflict." New York Times, 5 November 2012.

[79] "Medical Device Security." EECS 598-008, Winter 2013, University of Michigan. http://www.eecs.umich.edu/courses/eecs598-008/, last accessed 26 February 2013.

[80] Dan Auerbach. "4 Simple Changes to Stop Online Tracking." Electronic Frontier Foundation, 25 October 2012.

[81] Erick Bauman, Eva Galperin, Kurt Opsahl, and Peter Eckersley. "Don't be a Petraeus: A Tutorial on Anonymous Email Accounts." Electronic Frontier Foundation, 28 November 2012.

[82] Terms of Service; Didn't Read. http://tos-dr.info/

[83] Stephen Cass. "How to Talk to the Mainstream Media." The Last HOPE, 2008.

[84] "Private Browsing - Browse the web without saving information about the sites you visit." Mozilla, 2012. http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info, last accessed 20 January 2013.

[85] "DoNotTrackMe." Abine, Inc. https://addons.mozilla.org/en-us/firefox/addon/donottrackplus/, last accessed 21 January 2013.

[86] Ryan Gallagher. "The Threat of Silence." Slate, 4 February 2013.

[87] Adblock Plus. http://adblockplus.org/en/firefox, last accessed 20 January 2013.

[88] AdTrap. http://www.getadtrap.com/, last accessed 20 January 2013.

[89] Joe Martin. "Can You Erase Yourself from the Internet?" PC Pro, 11 February 2013.

[90] "China 2012 Crime and Safety Report: Bejing." U.S. Department of State Bureau of Diplomatic Security, 14 March 2012.

[91] Declan McCullagh. "Homeland Security: We Can Seize Laptops for an Indefinite Period." CNET, 1 August 2008.

[92] Elinor Mills. "Did Chinese Officials Copy U.S. Government Laptop Data and Use it in Hack?" CNET, 29 May 2008.

[93] Stephen Gandel. "ATM Crime: More and More Machines Get Withdrawn." Time, 7 October 2010.

[94] MobileScope, https://mobilescope.net/.

[95] Tom Simonite. "How to Detect Apps Leaking Your Data." MIT Technology Review, 10 August 2012.

[96] Finn Brunton and Helen Nissenbaum. "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation." First Monday, Vol. 16, No. 5, May 2011.

[97] Edward Sobiesk and Gregory Conti. "The Cost of Free Web Tools." *IEEE Security and Privacy*, May/June 2007.

[98] AFP, "Russian Unveils Secure 'Almost Android' Tablet to Keep Data Away from Google." Security Week, 31 August 2012.

[99] "Tor Browser Bundle." Tor Project. https://www.torproject.org/download/download-easy.html.en, last accessed 21 January 2013.

[100] "NASA to Encrypt Data After Its Latest Laptop Loss." BBC News, 15 November 2012.

[101] Eoghan Casey, Geoff Fellows, Matthew Geiger, and Gerasimos Stellatos. "The Growing Impact of Full Disk Encryption on Digital Forensics." Digital Investigation, Vol. 8, No. 2, November 2011, pp. 129-134.

[102] "EU Citizens Warned Not to Use US Cloud Services Over Spying Fears." Slashdot, 31 January 2013.

[103] Do Not Track. http://donottrack.us/, last accessed 20 January 2013.

[104] "FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers." Federal Trade Commission, 1 December 2010.

[105] "IOS Developer Cheat Sheet." The Open Web Application Security Project. https://www.owasp.org/index.php/IOS_Developer_Cheat_Sheet#Insecure_Data_Storage_.28M1.29, last accessed 21 January 2013.

[106] "HTTPS Everywhere." Electronic Frontier Foundation. See https://www.eff.org/https-everywhere, last accessed 20 January 2013

[107] Doug Gross. "Why the Interest in Illegal Cell Phone Jammers?" CNN News, 6 March 2012.

[108] Adam Bender. "Choice Urges IP Spoofing for Better IT Prices." Computerworld, 25 October 2012.

[109] Joe Grand, Jacob Appelbaum, and Chris Tarnovsky. "'Smart' Parking Meter Implementations, Globalism, and You." Defcon 17, 2009.

[110] Noah Shachtman. "Death by Algorithm: West Point Code Shows Which Terrorists Should Disappear First." Wired Danger Room Blog, 6 December 2012.

[111] "Camera Phone Predator Alert Act." Bill Summary and Status, 111th Congress, H.R. 414, United States Congress.

[112] Michelle Alexander. "Go to Trial: Crash the Justice System." New York Times, 10 March 2012.

[113] Adrian Kingsley-Hughes. "Are you following the NSA's 'Home Network Security Best Practices'?" ZDNet, 2 May 2011.

[114] "Camouflage from Face Detection." CV Dazzle. http://ahprojects.com/projects/cv-dazzle, last accessed 26 February 2013.

[115] Joshua Marpet. "Facial Recognition: Facts, Fiction, and Fsck-Ups!" Defcon 18, 2010.

[116] Tim Maly. "Anti-Drone Camouflage: What to Wear in Total Surveillance." Wired Design Blog, 17 January 2013.

[117] "Off Pocket: An Anti-Phone Accessory for Privacy Lovers." http://offpocket.com/, last accessed 26 February 2013.

[118] Benjamin Plackett. "Army Plots New Infrared 'Obscurants' to Thicken Fog of War." Wired Danger Room Blog, 5 October 2012.

[119] Katie Drummond. "Special Ops Wants Commandos to Have Invisible Faces." Wired Danger Room Blog, 18 November 2011.

[120] Speed Trap Sharing System. http://trapster.com/, last accessed 31 January 2013.

[121] Jakob Schiller. "License Plate Frame Foils Irksome Traffic-Light Cameras." Wired Raw File Blog, 19 October 2012.

[122] "Camoflash." http://ahprojects.com/projects/camoflash, last accessed 26 February 2013.

[123] Ari Ashe. "New Cameras to Watch Cameras that Watch You." WTOP News, 13 September 2012.

[124] Spencer Ackerman. "Suicidal Sensors: Darpa Wants Next-Gen Spy Hardware to Literally Dissolve." Wired Danger Room Blog, 28 January 2013.

[125] Brian Wheeler. "Give Social Networks Fake Details, Advises Whitehall Web Security Official." BBC News, 25 October 2012.